A Case Study of Mississippi State Penitentiary's Managed Access Technology

Eric Grommon, Ph.D.
Indiana University – Purdue University Indianapolis

Jeremy G. Carter, Ph.D.
Indiana University – Purdue University Indianapolis

Fred Frantz
Engility Corporation

Phil Harris
Engility Corporation

Engility Corporation, Rome NY
Award Number: 2010-IJ-CX-K023

August 2015

Table of Contents

List of Tables

List of Figures

Acknowledgement

The authors would like to thank Nancy Merritt, Joseph Heaps, Mississippi Department of Corrections, David Scott, Jack Harne, John Shaffer, Casey Joseph, Rick Pruitt, Peter Small, Charles Scheer, Eric Piza, and Anthony Salvemini for their support of this project as well as their insights throughout its completion.

Executive Summary

Contraband cell phone use in a corrections facility is an ongoing challenge for corrections agencies. There are numerous anecdotes of contraband cell phones being used to conduct criminal activities from inside a prison. Physical searches of inmates and correctional staff are limited in their scope; contraband policies and legal punishments possess deterrent value, but the effect of such approaches are not well known; and technologies to jam cell phone signals are in violation of U.S. law[1] and Federal Communication Commission (FCC) regulations. Recently, managed access technology has emerged as another approach to affect contraband cell phone use. This technology allows completion of authorized calls placed from approved phone numbers (numbers which have been vetted and entered into a database) while, conversely blocking calls to/from devices or numbers which have not been pre-approved; a process often referred to as "white-listing". The promise of this technology as an effective means to combat contraband cell phones has influenced correctional procurement decisions across the country. Yet, many unknowns exist with respect to its capability, functionality, and actual impact on contraband cell phone use.

The present research seeks to inform these gaps and provide corrections administrators and policy-makers with information describing managed access technology, its deployment, and relevant data on cell phone transmissions captured by a managed access system. A case study approach was used to learn about the Mississippi Department of Corrections' (MDOC) procurement and deployment processes used when they implemented managed access technology at the Mississippi State Penitentiary (MSP). A series of interviews and

[1] **47 U.S. Code § 333:** No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government.

teleconferences, in addition to the secondary analysis of managed access system data, were employed to generate a fundamental understanding of managed access technology operations, identify challenges and lessons learned, and develop a baseline of contraband cell phone activity. This assessment is not an evaluation of the operational efficacy of managed access technology. More specifically, the present study does not seek to quantify potential vulnerabilities or manipulations of managed access systems. Such an evaluation would be insightful, but is beyond the scope of the present study.

The present study identified the following challenges associated with deployment and operations of managed access technology:

1. Managed access has to be routinely "managed". This task requires a significant labor commitment from the host agency, in addition to ensuring that personnel have appropriate technical skills.
2. Managed access requires an effective self-monitoring capability.
3. The system must be designed to prevent illegal access to cellular signals originating outside the corrections facility, and procedures must be developed to address legitimate calls that are blocked by the system.
4. The signal strength of managed access system must be strong enough to cover areas in the facility while ensuring emissions do not exceed authorized levels or exceed authorized coverage areas.
5. Coordination is required with carriers and local public safety answering points to ensure proper handling of 9-1-1 calls.
6. Technology upgrades by cellular carriers can significantly reduce system effectiveness; close coordination with the carriers is critical for effective system operations.
7. The managed access system and associated physical infrastructure may be vulnerable to weather conditions.
8. Inmates may attempt to sabotage system infrastructure.

To address these challenges, and based on our observations, we note the following practices employed by MDOC:

1. Work with and educate representatives from the legislative community, the Executive Branch, and advocacy groups to advocate changes to existing laws and policies governing contraband cell phones.

2. Establish cooperative partnerships with cellular carriers.
3. Cross-reference captured phone call information with existing pre-approved list of inmate land-line numbers.
4. Treat managed access as part of a layered approach for counter-measures beyond traditional search capabilities.
5. Use managed access to eliminate inmate use of cellphone technology as a way to circumvent mandatory monitoring of inmate conversations, a condition of use associated with landline based authorized Inmate Calling Systems (ICS).
6. Use managed access to create a general deterrent to impact contraband cell phone market value.
7. Create a housing unit for contraband cell phone violators within MSP at Parchman.
8. Correctional facilities must harden managed access system hardware and associated infrastructure to prevent damage, system failure, and system inefficiencies from both inclement weather and premediated attacks by prisoners.

Despite these challenges, managed access technology does appear to detect and terminate a large number of cell phone transmissions. Our analysis of contraband cell phone activity data captured by MSP's managed access system and provided by MDOC for a five month period in 2012 yielded several useful insights related to the detection and termination of cell phone transmissions.

1. Not all blocked calls can be assumed to originate from contraband cell phones; any cell or wireless phone not on an approved caller list will be blocked by the managed access system operating at MSP.
2. A number of dial strings were identified during our analysis that did not correspond to telephone numbers associated with voice calls but instead represented system commands (e.g., #777, #768 etc.) associated with data services or phone configuration. These likely originated from contraband devices with CDMA[2] data capabilities that automatically query the network when turned on. An agency implementing a managed access system may derive additional information by analyzing captured managed access data resources,

[2] CDMA stands for Code-Division Multiple Access, a digital cellular technology. Tier one carriers Verizon and Sprint use CDMA technology in their 2G & 3G networks. Alternatively, AT&T and T-mobile use technology based on GSM (or Global System for Mobile) standards for their 2G/3G networks. These technologies, and their derivatives, are not interoperable. In addition to the tier-one carriers mentioned, there are approximately 50 regional CDMA and 70 GSM based regional carriers in the United States. An anecdotal but representative list of carriers can be found at http://www.ebay.com/gds/GSM-and-CDMA-Guide-/10000000009189079/g.html or http://www.unlockedshop.com/a-full-list-of-gsm-carriers-in-the-usa/ for a more comprehensive list of carriers. Note that these listings are subject to ongoing changes in the marketplace, in addition to interpretation by website authors, so they should be considered representative, but not authoritative sources.

a process that will require analysis of database content to determine context associated with a specific dial string (which may require additional information from carriers or other vendors). This finding also has implications for agencies in determining policies for managing the approved list.

3. While many unique device identification numbers were detected only once, some device identification numbers were detected over 1,000 times by the system over a period of months. This could indicate that even after a device has been captured by the managed access system, repeated call attempts originating from the same device and number are persistent, a condition which may indicate that inmates are probing to determine if the managed access system is not operating, or down for maintenance.
4. Patterns in call attempt data suggest that a significant amount of call activity was for the purpose of social contact. Increased transmissions were detected by the managed access system on specific days such as Mother's Day and federal or state holidays. Data on the patterns of call activity could not be used to identify or determine the frequency of transmissions to coordinate illegal activities.
5. The vast majority of documented/registered/captured contraband cell phone call attempts were voice calls (91%); the remaining 9% were texts.
6. The top-ten most commonly called numbers from inmates included cellular provider customer service lines, voicemail accounts, pay-as-you-go debit card companies, and a municipal library storyline for children. Most text messages were sent to private individuals.
7. Lastly, despite MSP personnel seizing slightly more contraband cell phones found in inmates' possession at Parchman compared to other MDOC facilities, fewer cases of contraband cell phone possession were forwarded to the District Attorney for prosecution that led to pending grand juries.

Limitations and assumptions for this report are provided in the concluding sections.

Introduction

Background and Context

Cell phone accessibility in the United States has been increasing significantly, due to a combination of lower cost technology and pre-paid plans. A recent report by the Pew Research Center (2014) estimates 90 percent of American adults currently own a cell phone. This trend is mirrored in correctional facilities nationwide as cell phones have emerged as one of the most prevalent forms of contraband within prisons (Burke and Owen, 2010; Worley and Cheeseman, 2006). As with any contraband in correctional facilities, true estimates of the problem are elusive. Recent spikes in the number of cell phones confiscated within correctional facilities have shed some light on the scope of the problem. For example, California Department of Corrections and Rehabilitation reported an increase of confiscated phones, from 900 in 2007 to 10,700 in 2010 (U.S. Government Accountability Office, 2011). Increasingly, cell phones are being confiscated in more secure facilities (U.S. Government Accountability Office, 2011)

The urgency to address contraband cell phones is driven in part by stories of violence and crime that are connected to inmate use of contraband cell phones in prison (see Appendix A). One such example is the attempted murder of Robert Johnson, the former captain in charge of finding contraband at the Lee Correctional Facility in Bishopville, South Carolina, where an inmate used a contraband cell phone to coordinate the attempted murder (CorrectionsOne, 2015). Gary Maynard, Secretary, Maryland Department of Public Safety and Correctional Service, summarized the complexity of the problem at a conference panel sponsored by NIJ (2010):

> When I first came here in January of 2007, the U.S. Attorney was investigating a homicide that occurred on the streets of Baltimore from a witness who was testifying in a criminal trial, and it was believed that that hit was called for by a Black Guerilla Family gang leader in a prison in Hagerstown, Maryland. That investigation did, in fact, conclude that that hit was called for. During that investigation, we found a lot of testimony that indicated that cell phones were being used for intimidation, drug

> distribution and many other criminal activities within the prison. We really have to target cell phones. The more we target cell phones, the more we learn about gang affiliations; the more we target the gangs, the more we find about cell phones. So they are intimately entwined in each other.

There are also ongoing Federal Communications Commission (FCC) activities and public debate on the cost of landline phones in prisons[3]. Contraband cell phones have emerged, in part, as a lower cost alternative to available landline phone plans. While recognizing that the factors that motivate contraband cell phone use are an open question and a relevant topic for future research, the focus of this study is the deployment of managed access technology to reduce contraband cell phone use.

Current methods to combat contraband cell phone use in correctional facilities rely on a combination of searches, sanctions, and technologies. Physical searches of inmates and correctional staff to find and confiscate contraband phones are limited in scope and often generate mixed results. The physical size of modern cell phones make them easier to conceal and they can be transported into the facility not only by people entering the facility but also as simply as being projected over a facility fence or wall. Contraband policies and legal punishments are implemented as a deterrent, but understanding their effectiveness is anecdotal and subject to interpretation. The number of technology based methods currently available to combat contraband cell phone use in correctional facilities is currently limited by regulatory and technology issues, as well as fiscal constraints, that create uncertainly in the decision-making process when choosing to deploy these systems. All forms of communications signal jamming, including the jamming of cellular communications within non-Federal jails and prisons, remains

[3] As this report was written FCC review of ICS (Inmate Calling Services) was underway. The FCC conducted a workshop in July 2014 regarding reform of inmate calling services. In September 2013 the Commission issued a Report and Order and Further Notice of Proposed Rulemaking in Docket WC 12-375 regarding rates of inmate calling services, and released a Second Further Notice of Proposed Rulemaking in that proceeding on October 22, 2014. For more information, see http://www.fcc.gov/document/fcc-continues-push-rein-high-cost-inmate-calling-0 and http://apps.fcc.gov/ecfs/comment/view?id=6017468678.

illegal by way of Federal law as outlined in the Communications Act of 1934 and other FCC rules (see FCC Jamming, n.d., and FCC 2005)[4]. Alternative methods currently used to address illegal cell phone use, such as phone-sniffing dogs and random cell searches, even when supplemented by detection technology are labor-intensive and typically yield less-than optimal results (U.S. Government Accountability Office, 2011).

Recently, a technology has emerged known as managed access. Managed access technology leverages core aspects of cellular technology by "managing" network services granted to a specific cellular user or cellular device. As with jamming technology, managed access technology actively transmits radio signals in many bands commonly used by commercial wireless providers[5]. Use of these bands is closely regulated by the FCC or NTIA[6]. In comparison, jamming technology simply disrupts ***all*** network communications denying service to all users[7]. Radio sensing technology is a passive alternative (i.e., receive-only technology does not require FCC authorization) in that it simply recognizes the presence of an active wireless uplink or downlink connection and then alerts the operator of its presence. As will be discussed in more detail to follow, managed access technology permits connections to/from approved phone numbers while intercepting and blocking call and other connection activity

[4] Federal agency authorization to use radio spectrum is not regulated by the FCC. Federal entities fall under the authorization of the National Telecommunications and Information Administration (NTIA). It is possible for federal agencies to request authorization to deploy and use cellular jamming technology via NTIA processes. The extent to which jamming technology has been authorized and deployed in Federal correctional facilities is unclear.

[5] Including bands associated with the Cellular Service, Broadband Personal Communications Service and certain Advanced Wireless Services.

[6] Note that the terms "active" and "passive", in context of regulatory and licensing discussion in this paper, describe technologies that actively transmit radio energy in commercial mobile service bands (active) or function as receive-only in these bands (passive). This is in contrast to use that describes operational use that "passively" disables the use of cellphones from a distance versus those that simply locate and then require "active" intervention on behalf of prison personnel to physically seize illegal devices. Both uses appear in this paper.

[7] The Communications Act of 1934, Section 333 - prohibits willful or malicious interference with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government (47 U.S.C. § 333). It is a violation of federal law to use a cell jammer or similar devices that intentionally block, jam, or interfere with authorized radio communications such as cell phones, police radar, GPS, and Wi-Fi, see http://www.fcc.gov/encyclopedia/jamming-cell-phones-and-gps-equipment-against-law

associated with non-approved, and presumably contraband, cell phones.[8] Managed access technology is one option to combat contraband cell phones, yet many unknowns exist with respect to its function, capabilities, and potential impact.

Purpose of the Technology Assessment

Given that managed access has been identified as a method to help control contraband cell phone use in correctional facilities, and corrections agencies have started to procure such systems, the purpose of this research is to provide objective, data-based information to inform procurement decisions. With this in mind, this study seeks to fulfill the following nine objectives:

1. Explain what managed access is and how it works;
2. Document the experience of the Mississippi State Penitentiary (MSP) with contraband cell phones and attempts to combat the problem;
3. Explain how managed access was installed and operates within the MSP;
4. Provide an empirical illustration of contraband cell phone use at the MSP;
5. Provide an empirical illustration of the effect managed access has on contraband cell phone use at the MSP;
6. Identify operational challenges of the managed access system in the MSP;
7. Identify lessons learned from MSP that facilitate managed access effectiveness;
8. Draw conclusions for policymakers based on available data and information gleaned from interviews; and
9. Provide guidance for future research on contraband cell phones and managed access.

Evolution of the Contraband Cell Phone Problem

Cellular Telephony and Services

There are currently four major nationwide carriers in the United States (AT&T Inc., Sprint Corp., T-Mobile USA, and Verizon Wireless), with some areas also served by unaffiliated

[8] We use the terms "call" and "connection" in this document interchangeably to describe a request for service placed from a cell phone. This service may be voice service, messaging services (text/email/multimedia) and/or Internet services that can be obtained from a contraband wireless device.

regional carriers.[9] Network operators use a small number of standard, but typically customized, wireless air interfaces, supported by a rapidly evolving technology base that drives a continuous cycle of system technology upgrades. Cellular services, in addition to basic telephony, include access to the Internet, and capabilities for users to communicate using text messages, video, images, sound files, and email.

Cellular telephony services and wireless data connectivity are provided by the wireless industry to end users through various types of contract mechanisms. For the purposes of this report, these mechanisms are grouped into two broad categories: post-paid and pre-paid contracts. Post-paid mechanisms typically consist of long-term contracts, of various types. In a typical consumer post-paid arrangement, cellular device cost is subsidized by the carrier. Monthly fees typically include a specific line item associated with the purchase cost of a specific cellular device, plus fees associated with basic wireless service and service options across monthly or multi-year contractual service agreements. Post-paid contractual information includes data associated with a well-known user, a specific wireless device, and a specific telephone number.

In contrast to services obtained via post-paid service agreements, pre-paid cellular encompasses a category of cellular services that are independent of constraints associated with typical long term contracts. Pre-paid service is often competitive with, or available at a lower cost than post-paid services, resulting in a rapid increase in utilization of such accounts.[10] Pre-paid service is available bundled with pre-packaged, off-the-shelf devices using the latest

[9] An anecdotal but representative list of carriers can be found at: http://www.ebay.com/gds/GSM-and-CDMA-Guide-/10000000009189079/g.html or http://www.unlockedshop.com/a-full-list-of-gsm-carriers-in-the-usa/ for a more comprehensive list of carriers. Note that these listings are subject to ongoing changes in the marketplace, in addition to interpretation by website authors, so they should be considered representative, but not authoritative sources.

[10] For more information see http://phys.org/news/2013-02-cellphone-users-prepaid.html

technology that can be user-activated without direct carrier interaction or a long-term service contract. Most importantly, for the context of this report, many inexpensive pre-paid devices can be activated over the Internet, anonymously, or with the use of false credentials. In a U.S. General Accounting Office (2011) report describing the use of illegal cell phones in Federal Bureau of Prisons (BOP) facilities, correctional officials noted the availability of less expensive cell phones as being a major challenge to the detection and confiscation of contraband cell phones.

Technology to Actively Manage Illegal Cell Phone Use

The National Governors' Association Center for Best Practices (2009) published a background paper outlining a number of approaches that are being taken by states to address the challenge of contraband cell phones, including detection, signal blocking, and punishment. The Department of Commerce (2010) published a study summarizing the results of a Notice of Inquiry into technologies to combat contraband cell phone use. Solutions proposed by industry to defeat the illegal use of cellular telephones included: technology to detect and locate contraband cell phones; radio frequency jamming technology and network-based capabilities that facilitate targeting and disabling of specific cellular devices; a subset which includes "kill switches" and managed access technology. In this section, we summarize these technologies in more detail, with emphasis on managed access technology.

As this report was written, nationwide institutional corrections community efforts underway to address the issue of illegal cell phone use were focused on changes to regulations that authorize (or prohibit) the use of technologies that actively disrupt operation of illegal cell phones in correctional facilities. These regulations are the subject of an ongoing FCC

proceeding (see FCC 13-58, 2013). FCC considerations include the potential establishment of guidelines, processes and timelines associated with spectrum lease agreements typically between wireless carriers and managed access system owner/operator. A common theme with each of the technologies under review by the FCC is the capability to remotely render cellular service ineffective through service denial, minimizing the utility of possessing an illegal device for prisoners[11]. This may simultaneously decrease the number of risks associated with personnel enforcing the rules through physical search while simultaneously increasing the risk taken by the smugglers who bring these illegal devices into a correctional facility. Detailed descriptions of ongoing regulatory activities are beyond the scope of this report because they have not concluded and the outcome of these proceedings remained uncertain at the time this report was authored.

Another significant FCC proceeding (FCC, 2012) established regulations associated with calling rate structures and regulations that define the rates correctional facility operators are allowed to charge for use of inmate landline calling services. As part of an FCC-sponsored workshop on the topic (FCC, 2010), correctional representatives testified that landline service revenues provide funding resources for programs used to counter illegal cell phone to include deployment of technology, in addition to revenues associated with inmate program support. Mississippi's Department of Corrections Commissioner noted: "…by them not using the landlines that we have done the best math we can and we feel like it is a couple million dollars. And those funds in my state, if I don't capture those, then I have to use taxpayer dollars to provide the teachers, the counselors, et cetera."

[11] With the advent of smartphone technology many devices can be used as standalone computing devices, cameras, or used with non-cellular radio technology (i.e., Wi-Fi or Bluetooth) for other limited wireless use. The FCC regulates aspects of these devices that relate to radio emissions and equipment authorization. FCC responsibility does not extend to how these devices are used for other purposes. Use of alternate wireless modes (Wi-Fi/Bluetooth) is not specifically addressed in this report.

Passive Sensing Technology

Unlike technology that actively emits, or transmits, a signal in the cellular radio bands, sensing-only technology represents a category of passive technologies (passive in context of *not* transmitting on "carrier-licensed" cellular frequencies.) Passive technology includes FCC authorized, and legally operated, unlicensed technology that supports physical detection of illegal devices. There is more than one type of sensing technology; metal detectors, magnetometers, x-ray technology, ferromagnetic detection, and nonlinear junction detection devices transmit on non-cellular frequencies to discover and locate electronic components in cell phones. RF signal detection is a listen-only sensing technology that employs radio receivers designed to listen to cellular frequencies and sense the presence of cell phone transmissions and/or determine the location of an active cellular device. These products are collectively "passive" with respect to licensed cellular frequency bands because in comparison alternative active technologies such as jamming and managed access are designed to actively transmit RF energy in carrier-licensed cellular bands, therefore they have significant regulatory and spectrum leasing implications. Unlike the technologies that actively disrupt cellular communications, users employing unlicensed passive sensing technology do not require specific prior FCC licensing, or cellular carrier spectrum leases.[12] Manufacturers of unlicensed equipment obtain FCC authorization for all products prior to sale.

Sensing technologies provide tools to assist with enforcement. Unlike technologies that effectively disable the ability to place voice calls or obtain other cellular data services from illegal cellular devices from a distance, sensing technology requires direct intervention by correctional staff to physically locate, confiscate, deny use of, or and analyze illegal devices.

[12] To clarify, active sensing or detection-only technology also exists. These devices actively ping contraband devices to obtain identifying information. These pings are active emissions and therefore these systems are subject to FCC licensing and, like managed access technology, require carrier spectrum lease agreements.

Institutions that use managed access technology typically use it alongside a combination of passive technology based tools to minimize the number of devices successfully smuggled into a correctional facility by screening visitors and employees as they enter a facility. The deployment and use of managed access technology in a real-world correctional setting is the focus of this report.

Jamming Technology

Jamming technology employs active transmitters that emit radio energy on cellular network frequencies; energy designed to disrupt all communication processes between network infrastructure and cellular devices. Jamming system signals used for this purpose need to be sufficiently strong enough to essentially "mask", or overwhelm, key components of wireless signals associated with nearby cellular networks. Jamming signals are indiscriminant, meaning that they disrupt all communications, including 911 calls, not just calls associated with specific devices or telephone numbers. As with managed access, poorly implemented jamming technologies are often strong enough to disrupt signals from nearby legitimate commercial network customers including public safety radios operating on nearby frequencies.

Deployment of this technology to combat illegal cellular phones involves detailed engineering design of a system tailored to each correctional facility as part of an implementation process. Inevitably, as with any wireless technology, there are variations in how jamming systems are implemented, and deployment specifics are highly dependent on the environment and specific jamming target. The end result is a blunt-force tool used to disable all cellular radio signals used for network connections. As noted above, current FCC policy is to consider all forms of radio frequency jamming to be illegal, including the use of jamming to counteract illegal cell phone use in correctional settings.

Network-based Technology: The Kill Switch

Network-based technology can facilitate targeting, and disabling, of specific cellular devices (i.e., activate a "kill switch"). A kill switch capability requires a two part solution; installation of intelligence into carrier network infrastructure alongside use of a "kill switch" function installed in *all* cellular devices sold in the United States. As with managed access this process relies on the success of processes to identify, capture and then ultimately deny the ability of a device to complete calls through a carrier's network. In current FCC proceedings (FCC, 2013), the cellular industry suggests that a kill-switch capability, developed primarily to protect consumers and combat the growing problem of stolen phones, should be a voluntary or opt-in technology[13,14]. This opt-in approach would obviously not work to combat illegal cell phone use in correctional facilities. Technical changes associated with kill switch capabilities need to be accompanied by closely coordinated policy and procedures that outline how correctional personnel can legally request, process, and then disable specific cellular devices; a complex process with unknown costs for all entities involved.

Ongoing debate in regard to policy and business issues associated with the use of both jamming and "kill switch" alternatives appear to be more challenging than underlying technical issues. The kill switch alternative would not require the installation of any active infrastructure at

[13] This kind of blocking technology is employed today by cellular carriers as an optional service to disable lost/stolen phones: For example, see http://newsroom.sprint.com/blogs/sprint-perspectives/sprint--at-the-front-lines-against-phone-traffickers.htm

[14] In August 2014, California passed a law to require a kill switch in new smartphones. The law was created to address the increasing problem of stolen smartphones; it is not designed to address correctional issues. Kill-switch processes would need to be further revised to address correctional enforcement needs. Considered in context of correctional issues, if the kill switch function defined in the CA legislation is activated by default in all new handsets, is likely that it would simply be turned off/disabled before a phone is smuggled into a prison. The CA law does not apply to feature phones, and the law verbiage specifies that it only applies to smartphones based on LTE and/or successor technologies, meaning that 3G smartphones using non-LTE technology are likely exempt. It also does not apply to second-hand phones. There are several aspects of the California law that limit its utility to addressing the correctional problem. See: http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0951-1000/sb_962_bill_20140812_enrolled.pdf

a correctional facility, instead requiring use of passive monitoring technology to assist in obtaining key information for identification and targeting of specific illegal cell phones.

Network-based Technology: Managed Access

Managed access, a term used here to describe a category of technology rather than a specific product, is an active technology. The FCC indicates that managed access products are in service, or authorized, in California, South Carolina, Texas, Maryland and Mississippi (see FCC NPRM 13-58 page 6, 2013). This technology is being deployed because, unlike jamming alternatives, it can be used within the bounds of current regulatory structure. Many aspects related to its implementation are currently under regulatory review to determine legal definitions, funding, specifications for deployment, adherence to cellular network spectrum lease issues, and carrier obligations related to ongoing changes in their networks. All of these decisions will affect managed access deployment and maintenance procedures.

To gauge the complexities of managed access from the perspective of network carriers, the Department of Commerce (2010) engaged cellular providers to assess their perceptions of managed access technology. A sample of the informative viewpoints is provided below:

> "Prohibiting access to the commercial cellular networks would solve 90-95 percent of all illegal communications within a prison…Verizon Wireless mentions that a managed access system can prevent phones from switching to other bands and would not need to intercept as many spectrum bands within prisons" (p. 20).
>
> "T-Mobile USA reinforces the effectiveness of a managed access solution in protecting public safety spectrum…a managed access system will provide more precise control over the bands selected for disruption, thus preventing interference with public safety wireless communication ….unexpected interference to other services is reduced" (p. 21).

> "The wireless providers – AT&T, Verizon Wireless, Sprint Nextel, and T-Mobile USA – all respond in favor of a managed access solution. This is due in large part to the system's ability to allow public safety, 9-1-1, and authorized calls to reach the cellular networks" (p. 21).
>
> "Verizon Wireless states that managed access can allow the system operator to maintain a list of approved callers – a list that can be amended constantly as subscribers that live, work, or frequently visit areas near the prison and are captured by the system are identified – whose calls will be allowed to [be] completed rather than blocked. Managed access systems allow prison officials, working with the system operator and nearby licensees, to set the parameters of how captured calls are handled. For example, prison officials can decide to allow the first call from a device not on the approved list to be completed, but block subsequent calls in order to prevent blocking calls from random subscribers near the prison, can decide to limit the duration of calls from non-approved callers, or can deliver a message to non-approved callers letting them know their call is being blocked by the prison system and advising them to move away from the prison to try again" (p. 22).

Anecdotal support, such as that noted above, is the only readily available currency upon which managed access can be evaluated by correctional officials who serve as potential consumers. This lack of reliable information is a result of the technology's recent emergence. Perhaps the most informed and well-articulated assessment of managed access to date is California Council on Science and Technology (CCST) (2012) report. This research was driven by California Department of Corrections and Rehabilitation's interest in a managed access system to combat cell phone problems in their facilities. Importantly, this study did not evaluate

an operational managed access system. Rather, investigators conducted focus groups with subject matter experts on the technology, reviewed vendor literature, system performance, and engineering information, and consulted experts in the field of corrections.

While the CCST report noted a number of interesting findings pertaining to contraband cell phones and prison security generally, the key findings related to managed access technology are highlighted here. Worth noting is that the report found glaring inconsistencies across physical screening at state prisons. This security shortcoming translates directly into the need for enhanced countermeasures within prisons such as managed access technology. Complexities of cellular signal capture were noted as a significant technological inhibitor of managed access to be implemented and maintained. A highly dynamic mobile industry that is driven by innovation and consumer demand makes it increasingly difficult to update mechanisms to capture signals and thus block calls.

The CCST report also noted concerns regarding the efficacy of managed access and its ability to be effective within the correctional environment. Specifically, "…managed access system technology today is not mature enough for immediate large-scale deployments…[and] specific protocols for success have yet to be defined" (p. 6). These concerns with managed access were noted as resulting from a lack of available evidence and baseline performance benchmarks of the technology. As such, the report closes with a call for the need to conduct independent research of an operational managed access system within a correctional environment.

The present report seeks to answer this call by providing evidence from the first operational managed access system in a prison in the United States. Next is a conceptual overview and technical description of how managed access technology operates. Following this discussion, the

case study approach is elaborated and the findings are presented. The report concludes with insights and recommendations for future research on managed access technology.

Technical Introduction to Managed Access Technology Concepts and Operations

In this report certain wireless concepts related to managed access of cellular technology are emphasized and described below. Concepts related to wireless interfaces and system coverage are independent of vendor-specific managed access implementation choices. For example, the architectural merits of distributed antenna technology and how they compare to alternative small cell technologies, and vice versa, are not addressed here. Nor are details of specific cellular provider networks and/or related cellular technology protocols. Each managed access technology product and deployment will be unique in many ways, dependent upon the local environment, regardless of the underlying managed access architecture. An examination of "features" associated with competing commercial managed access products are also outside the scope of this report. An overview of cellular system coverage follows, presented in the context of cellular and managed access technology. Managed access wireless system coverage, and how this type of system interacts with nearby commercial cellular networks is fundamental to all managed access deployments, regardless of which commercial managed access product is selected and deployed.

Cellular Technology

Cellular telephony, as a wireless radio service, functions much like other radio technologies. The use of radio technology, when boiled down to bare essentials, involves a process of inserting information of various forms into a radio transmitter which utilizes radio frequency energy to

convey the information through the environment wirelessly. As the wireless energy transits through the atmosphere and surrounding environment some level of radio signal degradation occurs due to a number of predictable and/or unpredictable factors prior to reaching a receiver. If the received signal is intact, a compatible receiver converts the information back into a format useful for its intended purpose. Protocols and procedures used to process the information during wireless transmission, and specific radio frequencies upon which the transmission occurs, vary. Some processes are based on open standards and others on proprietary technologies. Processes are also subject to specific engineering and business needs as radio network systems are developed and deployed. For example, commercial carriers Verizon, Sprint and AT&T each use wireless technologies based on 3GPP LTE standards, but their network wireless interfaces are different in many ways, and non-interoperable, because of specific implementation choices.

Cellular network operators are licensed and authorized by the Federal Communications Commission (FCC) to employ specific radio spectrum frequencies throughout specific geographical areas. Licenses are often granted following successful bids levied in a spectrum auction, often at a cost to a carrier measured in billions of dollars. In exchange for the proceeds from winning auction bids, the FCC grants the winning carrier exclusive use of frequencies so they can build network infrastructure and customer interface in the most optimal way to suit their business plans, as long as they do not exceed the technical and regulatory limitations associated with their licenses. Exclusivity means that they retain sole legal access to authorized spectrum, and this is a right that operators defend vigorously.[15] Any unauthorized signals emitted in carrier

[15] There are a number of Federal proceedings underway that are investigating ways to "share" spectrum, with a goal to more efficiently utilize limited spectrum resources. For example, FCC Docket GN 13-185, Regard to Commercial Operations in the 1695-1710 MHz, 1755-1780 MHz, and 2155-2180 MHz bands, is examining approaches to sharing spectrum between commercial and federal users; Docket GN 12-354 is considering commercial operations in the range of 3550-3650 MHz, currently used by federal users. If these efforts are successful, and commercial carriers are allowed access to new spectrum resources, or other spectrum users are

controlled spectrum space are considered to be interference by the carrier and the FCC. Managed access, considered as a category of technology, operates on these cellular carrier-exclusive network access frequencies to selectively disrupt cellular communications. This process requires close coordination with carriers to ensure systems operate in a legal manner.

For readers who are unfamiliar with wireless cellular technology, it is important to understand that there are constraints related to how wireless systems are designed and how they operate. Subtle differences are significant when considered in context of how managed network coverage is established and maintained. Many radio technologies, such as land mobile radios, are designed to operate in relatively quiet and interference/noise-free wireless environments. These radio services are typically designed to function with relatively few high-powered transmitters using antennas mounted atop tall towers to create networks engineered to operate in a relatively uncluttered radio environment, using technology relatively intolerant of radio interference. This type of network provides efficient signal coverage throughout an area using the fewest number of network sites, via the minimal amount of supporting infrastructure (i.e., additional base stations/repeaters). This is often referred to as technology operating in a "noise-limited" radio environment.

Commercial cellular radio infrastructure can be characterized by a few key distinguishing characteristics:

1. Cellular networks, similar to trunked land mobile radio technology, are bifurcated, composed of a network to customer air interface, often referred to as the "radio access network, or RAN" (i.e., wireless access to cellular towers/base stations) and a network backbone interconnecting the cellular towers;
2. Cellular networks are comprised of a relatively large number of lower powered base stations at cell sites designed with relatively low profile towers densely spaced in a way to efficiently support the greatest number of connections (i.e., users) via the customer

---

allowed shared access to cellular frequencies, the technical implications facing managed access technology may become very complicated.

wireless interface (i.e., the RAN) and/or to convey the largest amount of data through the access network by immediately offloading customer traffic from the RAN onto non-RAN network backbone connections (e.g., microwave radio, fiber optic cable, copper cable);

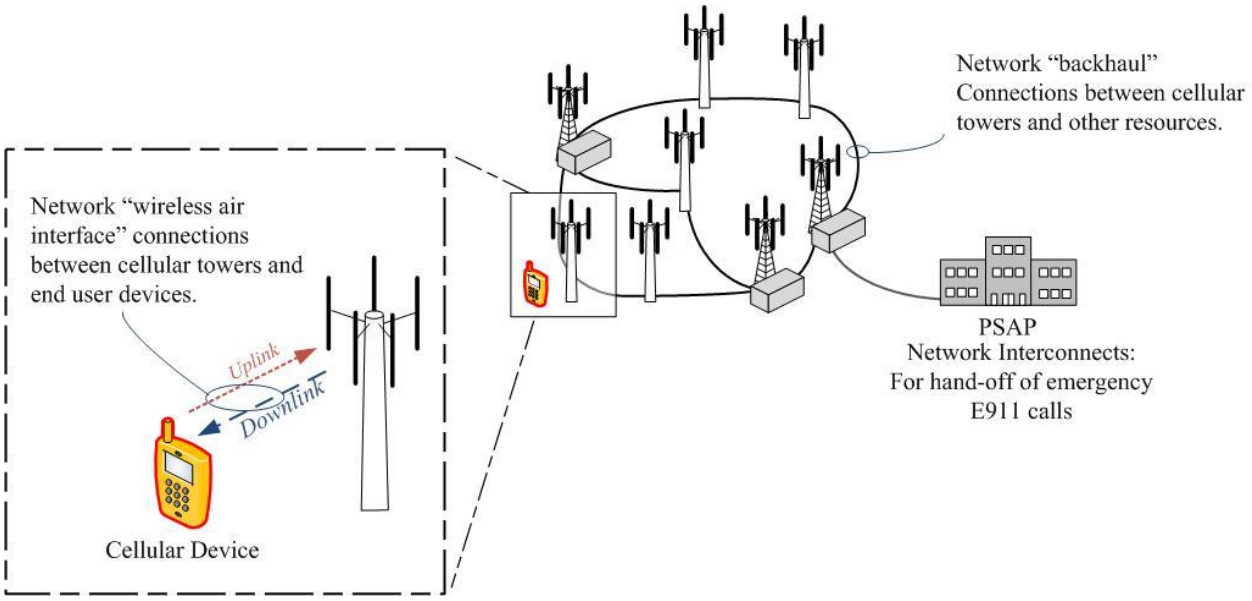
3. Cellular technology, similar to land mobile radio, must support mobility. Cellular networks are designed to support the movement of large numbers of relatively low-powered devices between cell towers that make up the RAN, while maintaining network and data connections, and;
4. Cellular access networks are constructed using a defined set of radio frequencies and a high level of frequency re-use and efficiency in the RAN (i.e., using the same frequency over and over again).

Because of the high level of frequency re-use, cellular technologies are designed to operate amid a relatively high level of radio interference created by adjacent cell sites. This is referred to as an "interference-limited" RF environment, whereby a baseline level of signal interference is expected, in exchange for increased levels of spectrum re-use and spectrum efficiency, driven by creating the greatest rate of return on a carrier's spectrum investment. Cellular base station density varies by business needs and typically mirrors the number of potential cellular customers; thus the number of base stations in an urban setting is typically greater and more densely deployed than the number of base stations in a rural setting where potential rate of return on investment is significantly less.

In a cellular environment, as with land mobile radio, wireless transmission occurs in two directions. Cellular transmissions from a base station radio transmitter, directed to receiver components within portable cell phone devices are often described as "downlink" transmissions. A transmission in the reverse direction, originating from a relatively low-powered portable transmitter (e.g., cell phone) directed to a base station receiver, is often referred to as an "uplink" connection. In a cellular network, the constraining wireless link is almost always the uplink between a low-powered end-user device and a network base station. If either the downlink or uplink connection components between a device and network fail, or become interrupted, then

communications to or from the cellular device will not work. Both managed access and jamming technologies rely on highly engineered systems to provide radio frequency signal coverage on cellular network access frequencies, but this coverage is required for quite different reasons. Jamming technology disrupts the communications path between the user and the network. Managed access does not; it depends on successful communications to first capture a wireless device and then grants or denies network services available to that device.

A managed access system is, fundamentally, a cellular network with limited scope and reach. A managed access network is designed to present the "dominant" network signal within its limited coverage area. Managed access networks are designed to operate using the same frequencies and protocols as those used by nearby commercial cellular carriers. Cellular devices, such as mobile phones, work by listening for a downlink signal, interacting with the strongest cell tower, and then automatically attaching to the network. A managed access system "intercepts" contraband cell phones by presenting a stronger network presence to a cellular device than nearby commercial towers do. Device to tower communications occurring via the RAN air interface uplink/downlink connections and network core should be further envisioned as having two distinct components: network signaling and customer traffic.



Source: Phil Harris, Engility Corporation

Figure 1. Cellular Network Concepts

Signaling transactions between the device and network that pass through the RAN are essentially part of a network management process used to identify and capture the calling device and then control service connections by requesting, establishing, reserving, and then releasing network resources as calls, data connection requests, or when inbound received calls are directed from the network towards a specific device. These communications are often referred to, collectively, as "overhead" communications. It is important to understand that wireless network backbone capacity is limited; therefore it is allocated to customers on an as-needed basis. Overhead communications associated with network and service management are constant and typically minimal in comparison to bandwidth required to support user voice or data communications. Managed access technology leverages the distinct split between network control and user connection aspects of cellular technology by "managing" network services granted to a specific end user or device. When a cell phone is turned on it initializes its operating system software, searches for and finds a compatible network and then connects to the strongest cell tower. Overhead signaling communications processes are used to "capture" and then direct

how the end-user cellular device interact with the network. This overhead process is used to identify the device, manage how the device interacts with the network (i.e., which tower, which frequency, device identification, user identification and service level) and to facilitate how services are delivered.

To phrase this differently, a cellular device "roams" onto the managed access system when it is operated within the managed access coverage area and becomes subject to local control, implemented via the managed access network which then manages service requests associated with devices[16]. Managed access system operations center around policy that defines which calls can be completed and which can be terminated. A managed access system provides the ability to selectively complete call requests made from select authorized phones or emergency calls from all phones, per facility policies and legal guidelines. In addition to blocking illegal calls, managed access systems also provide the ability to capture statistical data in regard to devices that attach to the system and/or data related to call attempts made from attached devices.

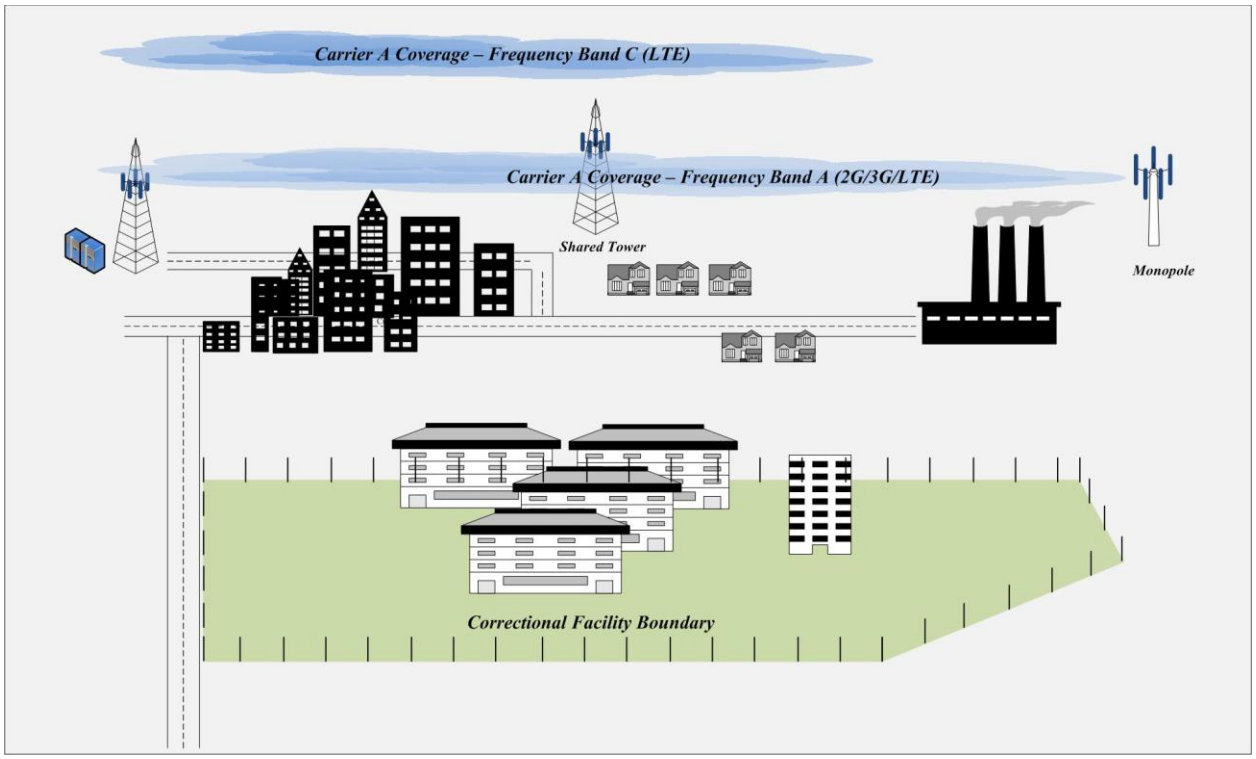
Managed Access Network Coverage

Wireless access network signal coverage envisioned from a simplified conceptual perspective can be depicted as an invisible cloud of radio energy at specific radio frequencies. The energy within a cloud associated with an entire network is additive, comprised of overlapping signals emitted from all antennas located on adjacent cell towers that use the same frequencies. Areas with inadequate signal levels are often described as "coverage holes"[17]. Transmitter components

[16] The term "roaming" is used loosely here; managed access systems actually appear to be part of the commercial network by presenting a valid commercial cellular Mobile Network Code to cellular devices. Outbound service requests are explicitly "denied" or "blocked". Inbound requests are also defeated because the managed access system does not make unauthorized phones visible to the commercial networks; therefore inbound calls to unauthorized phones connected to the managed access network cannot be completed.

[17] Note that the term "coverage hole" in context of commercial network coverage describes an area from which calls cannot be completed. A "coverage hole", in context of a managed access (or jamming) system describes exactly the

in a portable/mobile cellular device also emit a similar cloud of radio frequency energy that is centered on the current location of the device. How radio energy propagates through the atmosphere is predictable, to some extent, particularly in highly engineered cellular environments. For the purposes of illustration, carrier signals are depicted as different shades of color in the illustrations that follow.



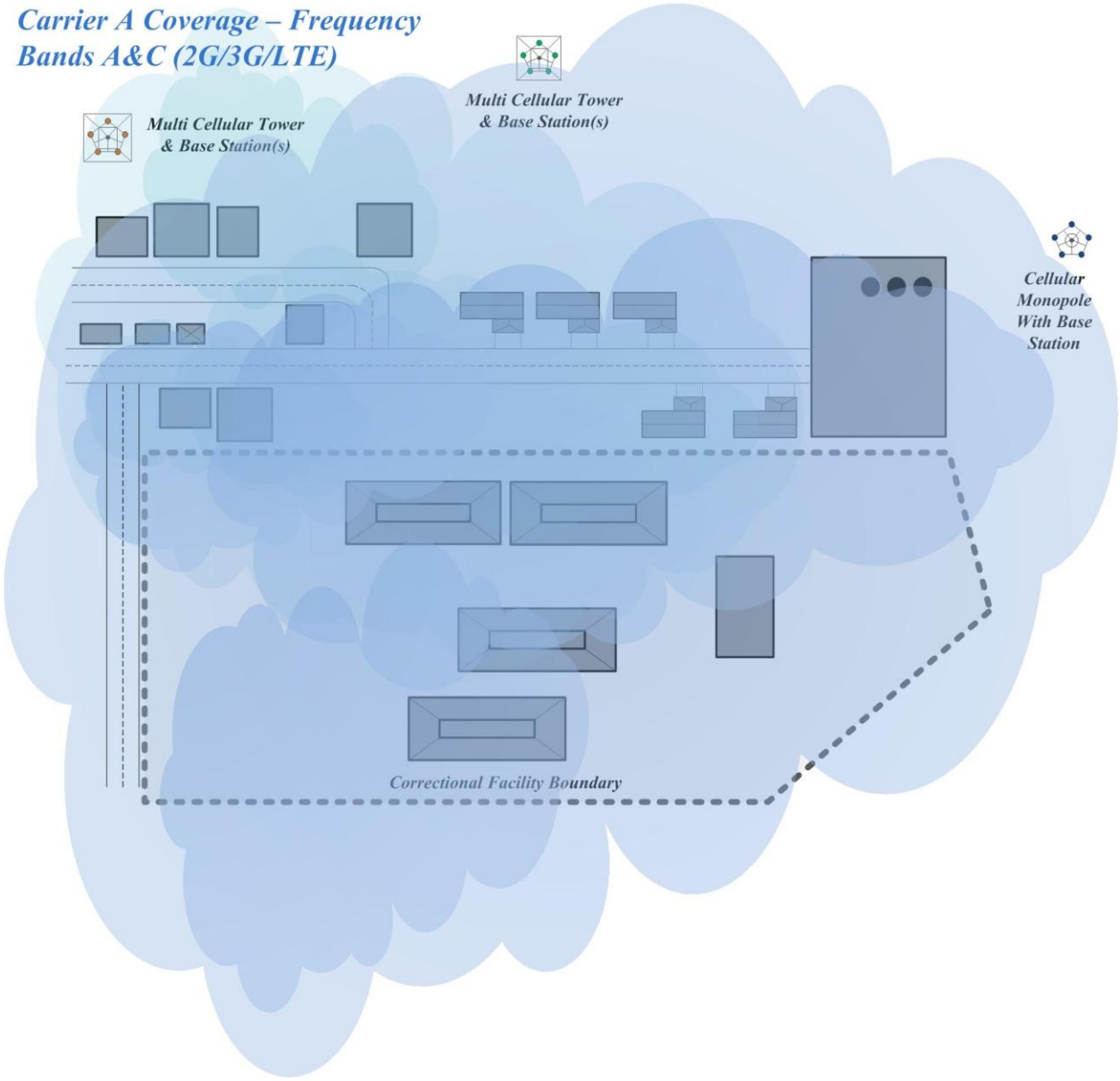
Source: Phil Harris, Engility Corp.

Figure 2. Conceptual View of a Correctional Facility and Nearby Environment

Figure 2 depicts a hypothetical correctional facility sitting adjacent to a town and residential area. In this example "Carrier A" provides wireless services throughout the town and surrounding areas, including wireless coverage that extends throughout the correctional facility. This cellular network operates on two different frequency bands (band A and band C, with

opposite, an area within the managed access footprint from which connection to a commercial network can be completed. Both describe locations with inadequate signal levels.

differing areas of coverage.) Figure 3 provides a top-down view of cellular network radio frequency (RF) coverage for carrier A in this setting.

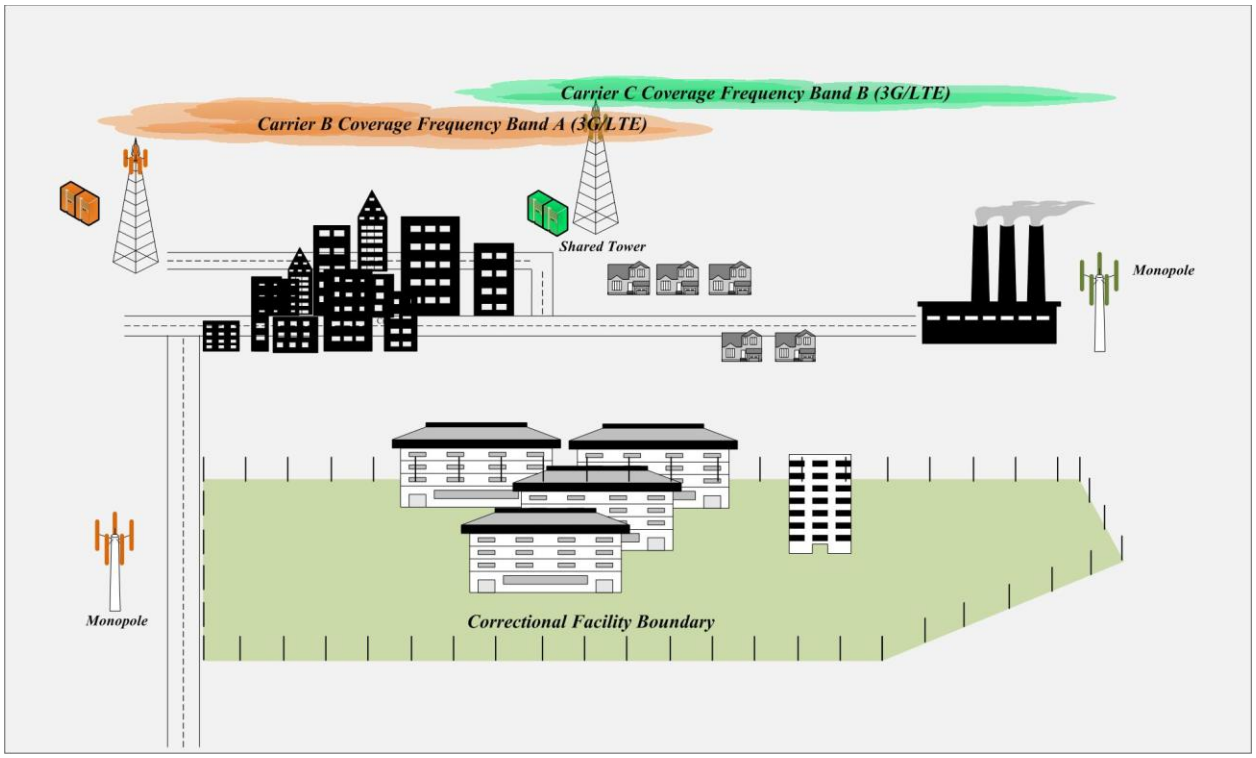


Source: Phil Harris, Engility Corp.

Figure 3. Conceptual Top-Down View of Signal Coverage from Cellular Carrier "A"

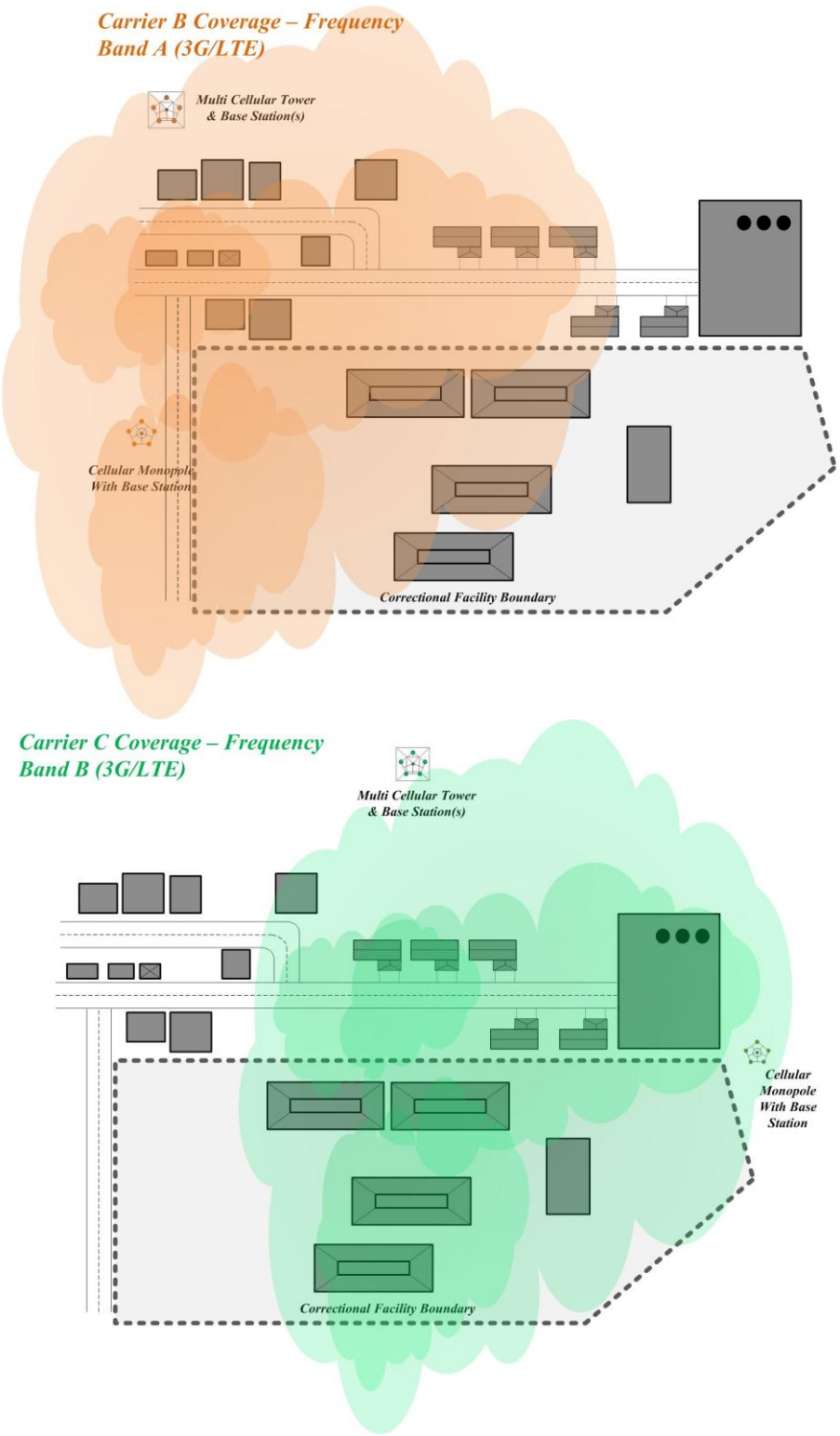
Two additional, competing, networks (B and C) are similarly depicted in Figure 4 and Figure 5. Coverage for each of these three cellular networks partially encompasses our hypothetical correctional facility. Each network is designed to provide a level of coverage suitable to the

operator's business model and customer base, using uplink design criteria associated with a typical portable device performance profile. Some level of inter-carrier resource sharing may occur when common network resources are used or when a tower is leased to two or more competing carriers. Although each network is unique, there is likely to be significant overlap in network coverage.



Source: Phil Harris, Engility Corp.

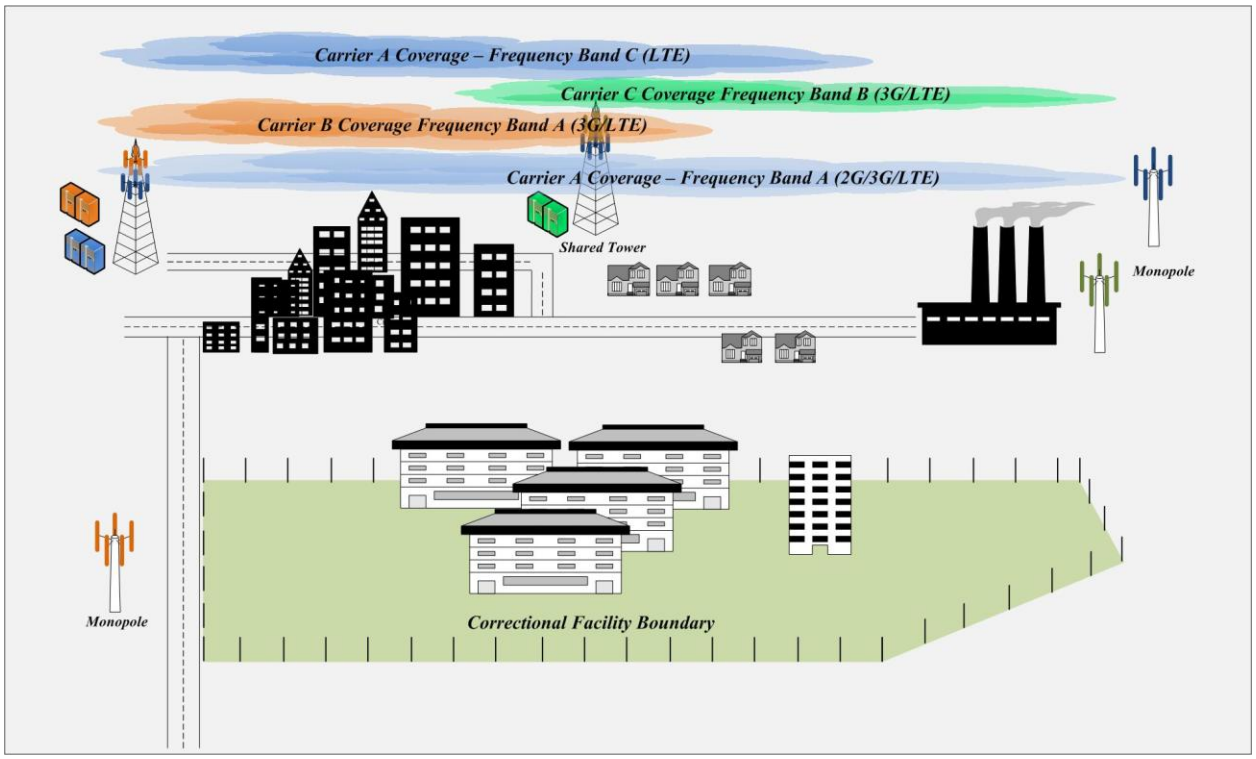
Figure 4. Conceptual View of a Correctional Facility and Carriers "B" and "C"



Source: Phil Harris, Engility Corp.

Figure 5. Conceptual Top-Down View of Signal Coverage from Cellular Carriers "B" and "C"

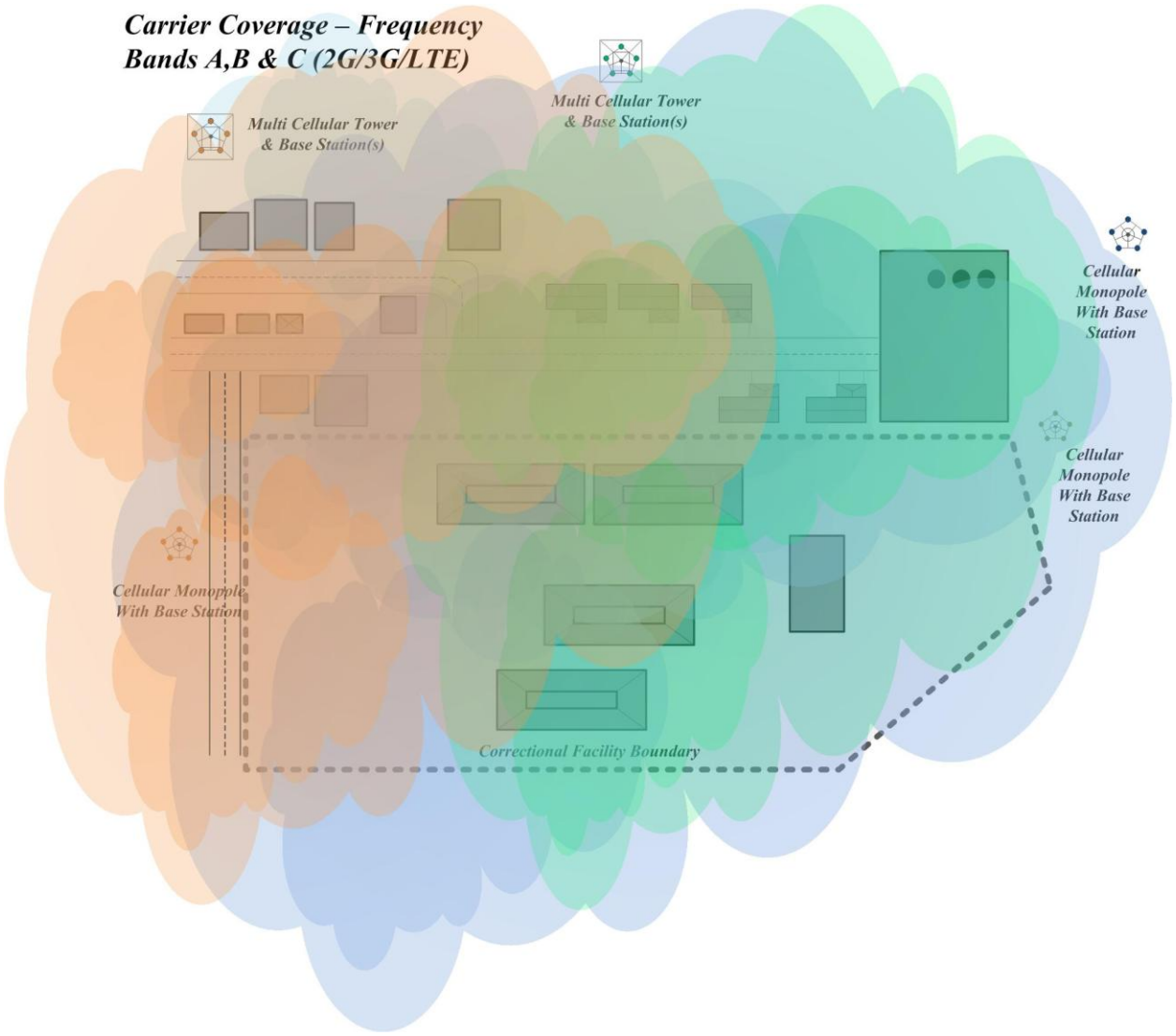
Figure 6 and Figure 7 combine individual carrier views to provide a single view of all three carrier networks. They are included to depict the complexity of the entire cellular wireless environment, and how combined cellular carrier coverage overlaps throughout the hypothetical correctional facility.



Source: Phil Harris, Engility Corp.

Figure 6. Hypothetical Correctional Facility with Carriers "A", "B" and "C"

It is important to acknowledge and understand this complexity as a combined threat, because any technology deployed to counteract illegal operation of cellular telephones in a correctional environment must, simultaneously, address the entire combined scope of devices connecting to all carrier networks.



Source: Phil Harris, Engility Corp.

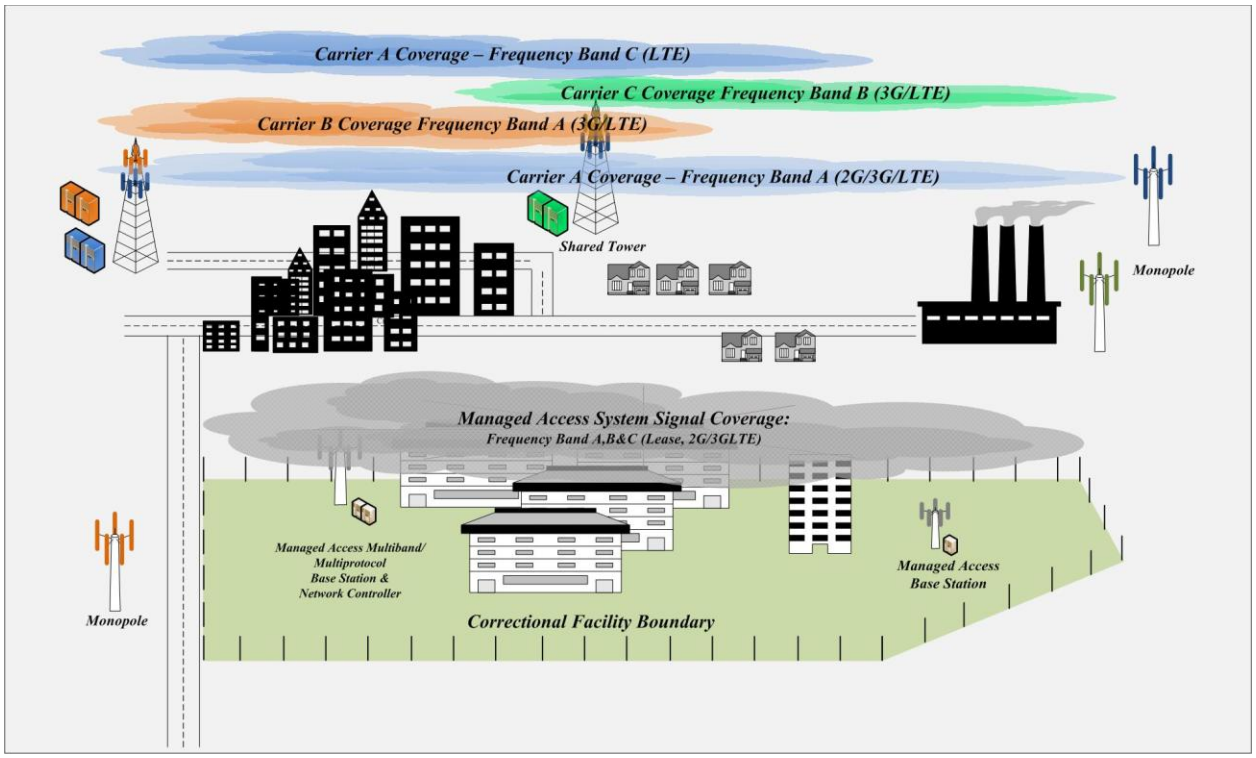
Figure 7. Conceptual Top-Down View: Signal Coverage: Cellular Carriers "A", "B" and "C"

It is important to note that the commercial carrier network environment is not static. Carriers have the freedom to change the topology and makeup of their network to optimize how their RAN interface frequencies and other network resources are used. Towers/network base stations, and carrier-specific network protocols are all subject to change as the commercial networks evolve. Commercial networks are not interoperable and must be addressed separately because different radio frequencies and protocols are used. For instance, Carrier A and Carrier B may both operate using the same frequency band, yet network devices may not be interoperable

because they have licensed and use different parts of the band. Network changes lead to corresponding changes in how cellular customer devices operate, and which uplink/downlink frequencies and/or protocols are used to support the services that they provide, and therefore network coverage changes as well. As noted above; as cellular operators make changes to their networks, the technology used to counteract the illegal use of cellular telephones must be adapted to ensure ongoing effectiveness. A correctional entity operating a managed access system or consuming services provided via a leased system must ensure that adaptations to counter carrier network changes are handled in a pro-active manner or the system will not retain its effectiveness as the surrounding cellular environment changes and new end user devices become available. Design, deployment, and operation of a managed access system is not a one-time event, it requires ongoing optimization and capability assessment in response to the surrounding environment.

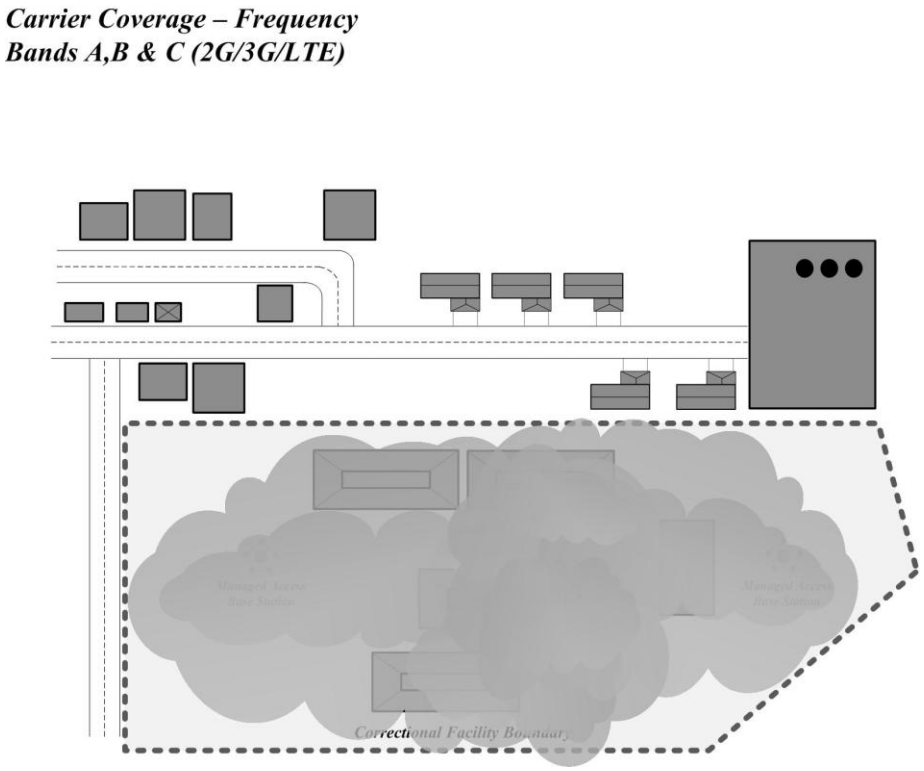
Capture and Roaming

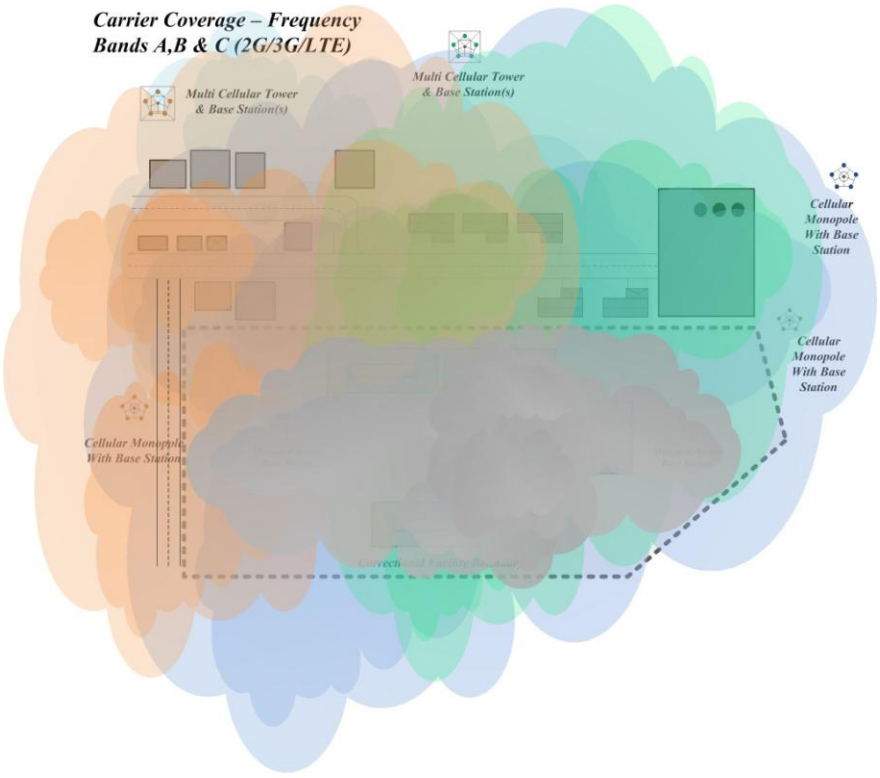
A managed access system is a multi-band, multi-carrier, cellular network of limited scope and coverage that presents itself as, and operates using frequencies leased from, each of the licensed commercial carriers. A managed access system emulates the protocols of each commercial carrier, simultaneously, so it can capture and control calls made using devices designed to work on all of the commercial carrier networks. Network coverage of a managed access system is designed to create and present a dominant signal on all commercial frequencies within a pre-defined area; typically defined by geographical boundaries established in spectrum leases established with each carrier and associated with an entire correctional facility, or at a minimum in specific areas where prisoners are present. This concept is illustrated in areas with grey shading, intended to depict managed access coverage in Figure 8 and Figure 9.



Source: Phil Harris, Engility Corp.

Figure 8. Conceptual View of a Correctional Facility with a Managed Access System





Source: Phil Harris, Engility Corp.

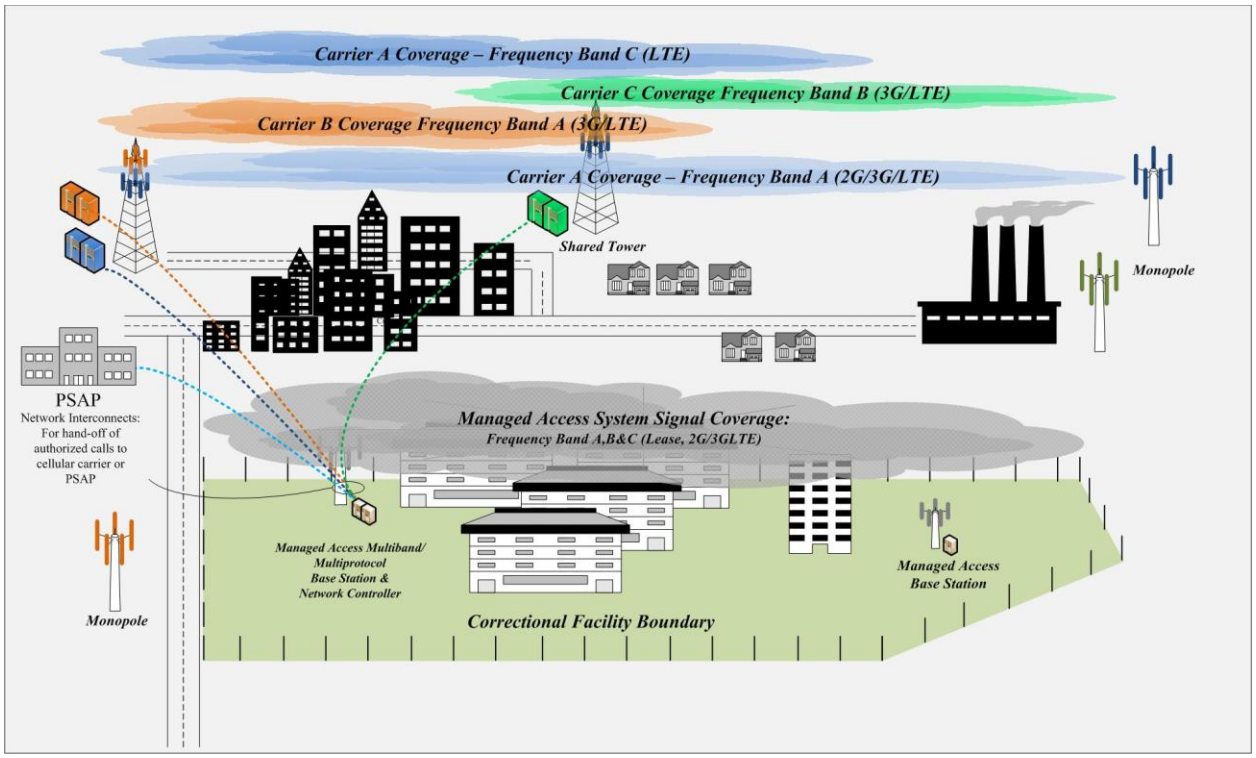
Figure 9. A Conceptual Managed Access System Network and Underlay

Managed access signal coverage is designed to overwhelm those emitted by the nearby commercial network towers. Another, perhaps more familiar, way to describe this process is to envision the managed access network as a cloud of radio energy that sits between illegal devices and the commercial networks. Cellular devices operating within the managed access "cloud" (coverage area) "roam" onto, and connect to the "managed access cellular network" instead of towers that are part of neaby commercial networks. This is analogous to, (but not quite the same as) roaming processes that occur between compatible commercial networks, because the managed access system is presented to the cellphone as part of the commercial network.

Once a connected device is captured, the "managed" aspects of the technology come into play. Disposition of calls originating from devices falling under control of the managed access

network is determined by state law, FCC regulations, correctional facility policies/regulations associated with operation of the network, and terms in the agreements established between the correctional facility and each of the comercial cellular carriers. Legitimate calls, such as those from authorized employees, or 911 emergency calls placed to Public Safety Answering Points (PSAP) can be handed off to cellular carriers for further processing, or routed directly to a PSAP. Implementation specifics associated with managed access are both deployment and system feature dependent.

Similar to network backhaul connections noted above, to support legitimate calls, some form of network connectivity is required between the managed access network and nearby cellular carrier networks, and/or directly to local emergency 911 centers. Implementation choices are subject to local implementation decisions and policies, Connectivity is acknowledged as simple network back haul interconnections in Figure 10. It is important to acknowledge that MAS design must consider both local policies and physical implementation of interconnections, and the recurring cost for these connections must be acknowledged as an ongoing operating expense.

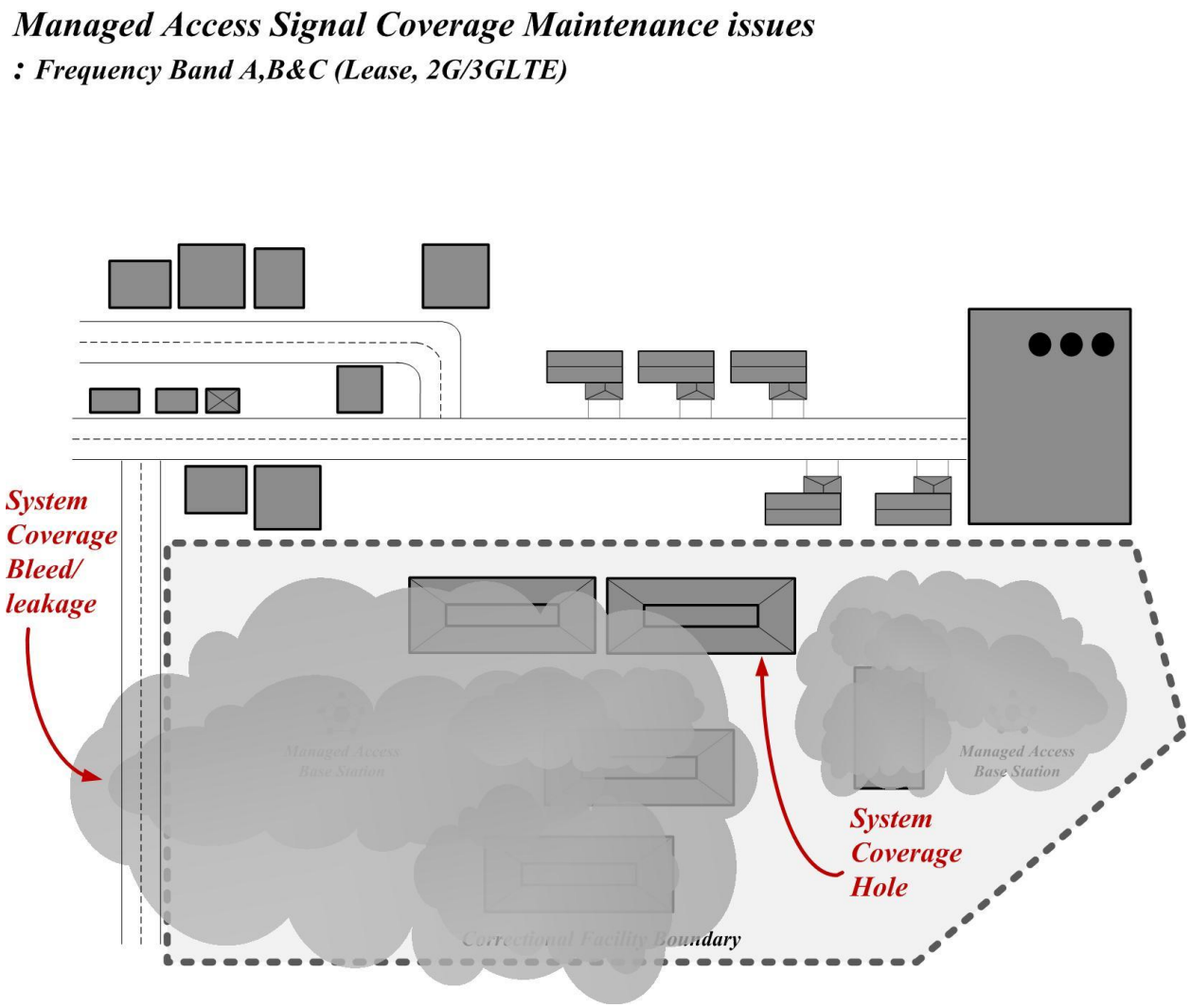


Source: Phil Harris, Engility Corp.

Figure 10. Managed Access System and Cellular System Interconnections

Coverage Related Maintenance

To comply with operational conditions defined within cellular spectrum leases, coverage must not extend beyond a well-defined service perimeter. System coverage changes can have significant impact on effectiveness if it creates coverage holes within the correctional facility. Correctional facility coverage holes can allow users to bypass the managed access system and access commercial networks. Conversely, signal leakage that extends coverage beyond the agreed upon managed access coverage area will lead to disruption of legitimate cellular users in areas where the managed access signal strength overwhelms coverage from a commercial cellular system operator.



Source: Phil Harris, Engility Corp.

Figure 11. Managed Access System Coverage Hole

Note that a managed access system operator has a *legal obligation* to ensure bleed-over does not occur beyond the defined coverage boundaries of a facility, in contrast to a*n operational need* to establish ubiquitous managed access coverage within that facility. Once constructed a managed access system is carefully activated and calibrated so that meets obligations associated with carrier spectrum leases and FCC rules to ensure it does not interfere with nearby commercial operations. After spectrum-lease lease obligations are achieved, the system can then be tested and further optimized to minimize any coverage holes to ensure expected operational effectiveness is realized within connectional facility. Ongoing compliance testing requirements

and methodology related to spectrum lease compliance may occur on a regular schedule, or in an ad-hoc fashion, depending upon spectrum lease details. Testing obligations and methodology used to confirm ongoing performance goals linked to operational effectiveness are subject to interpretation because these goals are not mandatory; therefore they must be documented in a concise technical manner by the deploying agency, and clearly defined as a requirement in procurement documents to ensure that ongoing operational testing requirements, costs, and associated obligations are well understood by both system suppliers and operators.

Coverage leakage can lead to FCC enforcement action and/or complaints and public relation issues. Coverage issues must be addressed as part of ongoing system maintenance. As previously noted, coverage changes may occur as a by-product of change within nearby cellular networks, or new capabilities introduced in commercial networks operated in areas adjacent to the correctional facility. For instance, a new commercial tower installation or a change in commercial network parameters (such as addition of a new band or protocol) can directly affect managed access system coverage[18]. Coverage issues may also result from infrastructure damage to either the commercial network or the managed access system as a result of weather damage or component failure. Any change that affects the relative balance between the strength of managed access and nearby commercial network signal strengths must be resolved.

This overview of managed access concepts and operations has described the conceptual functions of the technology and has identified some of the various factors that can influence system performance, establishing a foundation for subsequent research on user experiences with

[18] A managed access system design, to include carrier-specific managed access antenna placement, needs to address and optimize coverage for each carrier's frequencies; especially if the towers are not co-located or there are different deployment scenarios and each carrier transmits at different power levels.

managed access technology. The following section of the report will discuss the research approach used to generate knowledge about a managed access system deployment.

Methodology

The objectives of this research are to systematically document and provide insight into the implementation, operations, and potential impacts of managed access communication technology. Given the contemporary emergence of managed access system technology as a method to control contraband cell phone use in correctional facilities, the current research is exploratory in nature. A case study approach is most appropriate for this study since very little is known about the technology and the environment in which the technology operates is highly complex (Fitzpatrick and Sanders, 2003; Yin, 1994). A series of interviews and teleconferences, in addition to the secondary analysis of managed access system data, are employed to generate a fundamental understanding of managed access experiences, identify challenges and lessons learned, and provide insights on contraband cell phone activity.

In partnership with the Mississippi Department of Corrections (MDOC), a site visit to the Mississippi State Penitentiary (MSP) was conducted May 2012 in support of this research. Members of the research team included two criminologists, two communications engineers, and a senior policy advisor from the National Institute of Justice. Additional site visit attendees included individuals that were directly responsible for the implementation, management, and oversight of the managed access system. This included a law enforcement officer (MDOC), a managed access systems administrator (MDOC), a managed access system senior manager (MDOC), a technician from the MSP inmate calling system vendor (Global Tel Link), and a technology executive from the managed access system vendor (Tecore Networks).

During the site visit researchers administered a semi-structured focus group. Interview questions were targeted towards perceptions of managed access system usefulness in combating contraband cell phones, obstacles to implementation, successes, and areas in need of improvement (see Appendix B). King (1994) notes that semi-structured approaches are most appropriate for exploratory research as this method relies on open-ended questions that result from probing by the researcher and often times a free-flowing dialogue is created that guides the interview process. Detailed notes were taken individually by four members of the research team (two criminologists and two communications engineers) and then reviewed and transcribed into a single source document. To enhance the validity of interpretations from the site visit, additional teleconferences and continual communication exchanges with the Commissioner of MDOC and MDOC personnel occurred to solicit feedback, clarify and reaffirm the information gathered (see King, 1994).

Official de-identified aggregate data was provided by MDOC for secondary data analysis. These data were extracted from MDOC management information systems used to monitor captured transmissions from the managed access system and cell phone confiscations. Two sets of managed access system data are used. The first consists of the monthly count of all *call attempts* captured by the managed access system implementation in August 2010 to July 2012. The second data set includes daily counts of call attempts captured by the system across a five month period of March 2012 to July 2012. These data are a disaggregated sub-sample of the monthly count data and demonstrates the type of raw information captured by the system. In addition to the frequency of daily call attempts detected, these data include a variety of useful information. The type of call attempts detected by the system can be separated by signals using *call* or *SMS text* cellular functions. The managed access system captures International Mobile

Station Equipment Identity (IMEI) numbers, which identifies a unique cell phone device. IMEI serves as a measure of the number of *unique devices* that are responsible for generating signals. Finally, the system also captures the *destination number* or combination of numbers or keys dialed to place outgoing calls and SMS texts. The results are presented as descriptives.

It is important to note for the secondary analysis portion of this research that any call attempt captured by the system is assumed to emanate from an unauthorized, illegal, contraband cell phone. This assumption is informed by how the managed access technology system operates. Transmissions made from unauthorized cell phones are terminated and captured by the system, while transmission requests made from approved cell phones can be completed.

A third and final set of secondary analysis examines the case flow processing of contraband cell phone devices. Managed access system data were merged with internal MDOC cell phone confiscation reports from January to April 2012. This enables a brief "snapshot" comparison of case flow trends in confiscation and subsequent sanction and prosecution at MSP relative to all of MDOC's facilities. Confiscation reports include data on the number of confiscated cell phones found on inmates (*on person)* or *in common areas* of MSP as well as the number of *rule violation reports filed, cases forwarded to the district attorney,* and *cases with grand jury pending.* Data on the number of unique devices identified by the managed access system is only available for two out of the four month period. Descriptive results are presented.

Context: Mississippi State Penitentiary, Parchman Mississippi

Mississippi State Penitentiary (MSP)[19]

Mississippi State Penitentiary (MSP) is a maximum security facility located at the town of Parchman in Sunflower County, Mississippi. MSP is the state's oldest correctional facility, opening in 1901. Parchman is a rural area of northwestern Mississippi, and the facility encompasses approximately 18,000 acres. MDOC operates their Agricultural Enterprises division at MSP, which farms 6,300 acres of vegetables, rice, soybeans and corn. Figure 12 provides an overview of the location of MSP, reflecting both the geographic dimensions of the MSP property and setting. The red line shows the approximate boundary of the penitentiary. The circle in the interior indicates the MSP water tower that serves as the primary managed access system antenna system support structure. Subsystems are installed within all of MSP's inmate housing units. All of the units are identified by their unit number, except for the Hospital (Unit 42).

[19] Information presented in this section describing MSP was gleaned from annual Mississippi Department of Corrections reports (see Mississippi Department of Corrections, n.d.).

Source: Google Earth, with annotation by Fred Frantz and Pete Small, Engility Corp.

Figure 12. Mississippi State Penitentiary Grounds

MSP has a capacity of approximately 4,648 beds and its infrastructure includes fifty-eight support buildings. MSP has seven different housing units, ranging in size from fifty-six beds in the hospital to 1,521 beds at a primary farming support unit (Unit 29). Only male offenders are housed at MSP. Custody levels managed at MSP include offenders assigned to minimum, medium, and close restricted security classifications. All offenders classified as protective custody, administrative segregation, and death row are housed at MSP. Definitions for these classifications are provided in Appendix C. Mississippi State Penitentiary operations are administered by management staff consisting of a superintendent, three area-based wardens, and five deputy or associate wardens. There are approximately 850 security and non-security employees at MSP.

The facility's capacity was reported to be 4,648. To provide context of the inmate population managed by MSP, Table 1 illustrates total annual inmates populations (as of June 30 each year) for the MDOC and the U.S. as a whole. The overall incarcerated population trend for the MDOC is consistent with state-level incarceration trends across the nation. Incremental increases are observed since 2000 that have been stabilizing in recent years. The population of offenders housed at MSP has been declining since 2000. Fifteen percent of the total incarcerated population managed by MDOC is housed at MSP.

Table 1. MSP and MDOC Offender Populations

Year	MSP	Total MDOC	Percent of MDOC Population at MSP	US State Average of Total Incarcerated
2000	5,229	18,005	29%	38,770
2005	4,340	20,085	22%	43,900
2010	3,261	20,774	16%	45,402
2011	3,055	21,021	15%	44,812
2012	3,354	21,860	15%	44,568

Source: Mississippi Department of Corrections (2014a) and Bureau of Justice Statistics (2013).
Note: US State Average of Total Incarcerated inmates was calculated as the total national population of incarcerated inmates divided by 50.

Findings

Findings are presented in the following three sections. The first section, "Contraband Cell Phones in Mississippi State Penitentiary," provides insight on MDOC's experiences managing the contraband cell phone issues at MSP. The next section, "Managed Access Operational Challenges and Lessons Learned." will identify and discuss both operational challenges and lessons learned from the managed access installation at MSP. These first two set of findings were noted during the site visit and from numerous teleconferences and email exchanges with key informants and stakeholders involved with the managed access system deployment at MSP. The final section, "Contraband Cell Phone Activity," presents descriptive results of MSP's managed access system data. These findings pertain to captured cell phone transmissions from

within MSP and also provide profiles for select mobile devices operating within MSP to illustrate device usage. This section also begins to explore preliminary outcomes on the effect of managed access system on cell phone confiscations. Important limitations and assumptions of these findings are noted in the concluding sections of this report.

Contraband Cell Phones in Mississippi State Penitentiary

Extent of Problem. It is difficult to quantify the extent of contraband cell phones available. MDOC representatives estimated that approximately 25% of the total incarcerated population at MSP was believed to have been in possession of a contraband cell phone. Using the most recent data available on MSP's total inmate population (see Table 1), this equates to 838 inmates in 2012. MDOC, like most states, did not begin keeping record of contraband cell phones confiscated until 2007. For the year 2008, 2,214 contraband cell phones were recovered at MSP. This number grew to over 3,400 in 2013 (Mississippi Department of Corrections, 2014b).

There are a variety of factors that are influenced by the presence and use of contraband cell phones. MDOC representatives noted that cellular devices were being used to gain unapproved phone and Internet access privileges. Importantly, these cellular communications cannot be monitored or recorded. There are documented instances across the nation that these devices are also used to participate in criminal activities including drug dealing, planning and assisting escapes, extorting, threatening or ordering violence against a public or private citizen, and harassing crime victims. The potential for continued criminal behavior is one of the main concerns among focus group participants. Additionally, contraband cell phone use also affects state budgets and Mississippi taxpayer burdens. The use of contraband cell phones reduces the need for designated inmate phone system use, which decreases the amount of revenue available to MSP to support treatment and welfare programming.

Means of Obtaining Contraband Cell Phones. MDOC representatives indicated that MSP's contraband cell phone challenge is associated, at least in part, with visitors and correctional staff members that are paid by inmates to covertly smuggle contraband cell phones for inmate use. MDOC personnel estimate the market value for a contraband cell phone at MSP to range from $300 to $1,000 per phone; which makes these devices valuable commodities.

A critical issue for MSP administrators has been the recruitment of MSP correctional officers. MSP is the largest employer in Sunflower County; a county with a 15% unemployment rate which is twice as high as the unemployment rate for the state of Mississippi as a whole (U.S. Department of Labor Statistics, 2015). It was stated that the location of the MSP facility limits the correctional officer employee applicant pool, making it difficult to select highly qualified personnel to fill necessary vacancies and maintain the security of the facility. Similarly, the entry level salary offered to correctional officers has the potential to incentivize contraband cell phone smuggling. That is, the sale of one cell phone has the potential to provide multiple days' worth of wages as correctional offices across Mississippi earn an average wage of $13.88/hour (U.S. Department of Labor and Statistics, 2013).

As noted, MSP is located in an expansive rural area. MDOC representatives discussed instances in which citizens have thrown or catapulted cell phones over outer MSP perimeter barriers. MSP inmates also spend a significant amount of time working for Agricultural Enterprises and/or performing community services to local municipalities, counties, and state agencies. All of these factors provide opportunities for a contraband cell phone to be accessed by an inmate.

Toward a Managed Access Solution to Combat MSP's Contraband Cell Phones. MDOC examined a number of potential alternative technologies as tools to assist in the battle to control

illegal cell phone use that would supplement their procedures for contraband searches of persons entering the facility. MDOC deployed and continues to use canine teams to detect and confiscate cell phones. MDOC and also explored several products/systems designed to identify the presence of phones, including passive cell phone detection technologies. There were a number of concerns with these technologies when they were piloted including:

- Products interfered with officers' radios.
- Products disrupted cell phone communications of MSP employees who reside on the grounds of the facility.
- Products generated false detections, particularly around coax cables.
- Products did not perform well due to materials used in prison construction.
- Products provided detection, but not location information.
- Portable products were bulky, and their use could not be concealed, reducing their effectiveness.
- Manual searches were still required upon detection, which were labor intensive, disruptive, and exposed officers to potential safety issues.

MDOC considered additional approaches to physically blocking the introduction of cell phones into the facility such as body scanners and large nets around the perimeter and concluded that additional measures were required. While MDOC was assessing various passive detection technologies, it was noted that the Commissioner received an advertisement for a managed access technology product. This information was passed to Global Tel Link, who held a contract to be MDOC's designated landline phone service provider. After reviewing information pertaining to a similar system deployment in a Puerto Rico prison in December 2009, MDOC administrators determined that managed access provided the capabilities needed to affect

contraband cell phone use in their facilities. MDOC indicated that the managed access system at MSP was subsequently procured from Tecore on an expedited basis by Global Tel Link, and then installed, and made fully operational by Tecore in August 2010. MDOC supported the Global Tel Link deployment process by providing physical infrastructure required to support the system, to include AC power, fiber optic cable, concrete slabs and other items. MDOC representatives noted that that the brick and mortar aspects of the system deployment were completed quickly and the system provider (Tecore) noted that that the foundation for legal framework associated with spectrum leases had been well underway prior to this deployment. Significant details in regard to what happened in the first six or seven months in 2010, or in what order things happened were not provided. The fact that the MSP design is a single site system, which uses an existing water tower as the primary antenna support, certainly facilitated an accelerated deployment.

Tecore Networks is the MSP managed access network technology provider. Tecore's technology foundation is a product referred to as the iCore®, a software defined all-IP core network component with a scalable software architecture that provides functionality compatible with large commercial systems. The iCore® product provides support for current 2G, 3G, and 4G cellular technologies with claims to be upgradeable in support of future 5G technologies.

Managed Access Operational Challenges

A number of operational challenges experienced by MDOC personnel while deploying and operating a managed access system at MSP were identified. These challenges are presented to inform practitioners and vendors alike. The former should be conscious of these issues leading up to, or perhaps in the wake of, a procurement decision. The latter should take these challenges

into consideration when evaluating their product delivery and maintenance services. Table 2 provides a summary of the operational challenges of managed access found in MSP.

Table 2. Summary of Operational Challenges and Associated Issues

Operational Challenge	Issues Associated with the Challenge
1. Managed access has to be routinely "managed"	• Creation and updating of approved "white list" phone numbers
2. Managed access must include an effective self-monitoring capability	• Without telemetry and self-monitoring features a system will not alert the operator about equipment or component failure leading to fluctuations in signal strength. • The MSP system does not automatically self-adjust signal strength.[20]
3. Signal strength of managed access systems - signal bleed over	• System signal coverage must be routinely checked to ensure the signal remains within the designed coverage parameters and spectrum lease conditions outside the facility. • Phones outside prison facility can be captured by system, resulting in blocked calls from legitimate commercial users.
4. Signal strength of managed access systems – coverage holes	• Coverage must be routinely checked to ensure the signal strength is dominant within the facility to remain effective. • If competing signal strength from a nearby commercial network is stronger, illegal cellular call attempts may bypass the managed access system and create system coverage holes.

[20] This may be true of other managed access products as well. Implementing a system capable of self-monitoring and adjustment of signal strength for lease compliance would require a network of permanent sensors throughout the periphery of the correctional facility operational area (e.g., lease area) constantly assessing signal levels to ensure bleed-over does not occur. Similarly to optimize effectiveness inside the periphery, a network of sensors would be required within the correctional facility to assess coverage. Both of these "sensor networks" would feed an automated system to monitor and adjust signal levels; not impossible, but a capability that would significantly increase system costs. For this reason, ongoing MAS maintenance procedures, to include signal level maintenance, must be defined as part of the ongoing cost of ownership.

Operational Challenge	Issues Associated with the Challenge
5. E-911 call management	• Requires cooperation with both cellular carriers and local Public Safety Answering Points. Implementation varies by vendor and local requirements; Tecore directs 911 calls to public safety answering.
6. Technology upgrades by cellular carriers can significantly reduce effect system effectiveness.	• Managed access technology must be in sync with the technology deployed in nearby commercial networks. • Failure to do so will result in system coverage holes, create coverage bleed over, or simply allow callers to bypass the system.
7. Managed access systems should be hardened to resist damaging weather conditions.	• Antennas need to be adjusted after strong winds to restore proper coverage. • Commercial electrical power brown outs effect signal system performance.
8. Managed access systems should be hardened against sabotage: Inmates may attempt to sabotage system infrastructure.	• Inmates at MSP had attempted to cut exposed cables as well as drive a field tractor into managed access infrastructure.

Managed access must be routinely managed. MDOC stated that they anticipated the system would be a "plug-and-play", based on vendor information; however unexpected real-world elements came into play that changed initial expectations in regard to how the system should perform. MDOC stated that occasional system maintenance-related performance issues are addressed as they occur. MDOC stressed that confirmation of the coverage area was an ongoing maintenance task. MDOC personnel indicated that they did not anticipate the resources required to maintain and manage the authorized caller database. It was unclear what specific personnel were permitted for inclusion on the approved call list at MSP. No policies with respect to organizational rank or position for inclusion on the approved list were observed. Once this approved phone list was created and integrated into the managed access system, this approved list was constantly in need of updates to add or remove authorized devices as personnel were

hired, given access, or were no longer employed at MSP. No estimate was provided with regard to the frequency of occurrence of this task at MSP, just that it was "a regular occurrence."

MDOC emphasized that "managed access is 'managed." These sentiments were reiterated throughout the course of discussions. An over-arching, and generic concept that is critical to the operation of managed access systems is the fundamental capability to distinguish between telephone calls that will be blocked by the system from those that will be permitted (i.e., what other types of communications, such as instant messages or emails, will be passed through the system). As noted above, the goal is for all compatible cellular devices within system coverage to connect to the system so that call completion procedures and data service requests can be processed through the managed access system: therefore only authorized calls or data connection requests are successfully processed through the managed access system. To be successful, information about authorized users must be known in advance and pre-configured into the managed access system database. Once a cell phone connects to the managed access system it is captured by the system, and those not configured in the database are denied service. For voice calls, the system intercepts and blocks the call service requests. A voice notification advises callers that it is a felony to use an unauthorized cell phone device within the facility. Unlike intercepted voice calls, no feedback is provided to a user if a text message is blocked by the system; unauthorized data/text service requests are simply terminated and not completed by the managed access system.

Global Tel Link telephone analysts work with MDOC to implement and maintain a database to identify devices from which authorized communications can be made once the device connected to the managed access system. Global Tel Link also records and maintains data generated by the systems that can be used to identify unauthorized call attempts from illegal

cellular devices that have connected to the managed access system. They also generate various managed access reports using data captured by the system. MDOC noted that data stored in confiscated phones include activity logs which can be compared against event logs created and stored in the managed access system. This data can be correlated to assist in identification of system maintenance-related issues. Correlation of these data sets can be used as a tool to identify times when an increase in completed calls occurred, which may provide an indication that the managed access equipment appeared to be malfunctioning or inoperable, confirming a need for system maintenance.

Managed access must include some self-monitoring capability. Global Tel Link employees are responsible for overall general system maintenance. MDOC indicated that Global Tel Link initially monitored system operational status remotely and that information in regard to operational status to include notifications about system impairments, or equipment outages, were not always passed to MDOC from Global Tel Link. As a result system monitoring procedures were modified to add requirements for on-site technical support personnel, and adjustments were made to system fault information reporting procedures to ensure that information is passed to the MDOC Electronic Surveillance Center which monitors the facility's security and operations via closed circuit television.

Further complicating challenges associated with operating the MSP managed access system was the absence of an effective telemetry, or self-monitoring capability to detect equipment failures within the system. At the time of the site visit, system performance was measured by technicians as part of a routine scheduled maintenance program. This implementation lacked mechanisms to self-diagnose equipment failures that may lead to fluctuations in signal strength or inoperable equipment. This diagnostic shortcoming was compounded by the issue of adverse

weather. Weather issues at MSP were significant enough to warrant inclusion in this report to raise the issue for both practitioners and vendors of managed access[21]. System requirements should be specified in the procurement process mandating that components be hardened sufficiently to withstand harsh weather conditions experienced at the correctional facility. Note that, for example, that an antenna which is misaligned as a result of a weather event may remain fully operational, but MAS transmission (and reception) would be pointed in an incorrect direction. This would result in unexpected changes in system coverage area resulting in signal bleed-over or unexpected coverage holes.

Signal strength of managed access system and signal bleed over. Coverage within facility bounds is directly, and solely, related to system effectiveness and how it meets the needs of its operator; in other words operators with nearby facilities may have little interest in how a managed system performs as long as it does not impact their network. System coverage beyond the boundaries of the correctional facility will effect nearby commercial network users, and coverage bleed-over is also related to lease and regulatory issues.

Core MSP managed access system components are housed in a telecommunications shelter that sits adjacent to the MSP water tower which is centrally located in the correctional facility. The water tower serves as the primary managed access system antenna support structure. The system also includes subsystems that extend, or improve, coverage within all seven of MSP's inmate housing units on the grounds of the facility. It was noted that subsystem installations required engineering and construction of conduits routed through areas within the buildings to

[21] At the time of this report, there were two news reports of weather-related system outages at Parchman, one in August-2010, and a second one in March 2014 that resulted in inmates sending images via illegal cell phones. This is documented as a news item at http://raycomnbc.worldnow.com/story/24945407/exclusive-contraband-phones-inside-parchman

ensure that cabling would be isolated to minimize vulnerability to inmate tampering. Appendix D provides additional information concerning MSP infrastructure.

When the MSP system was initially installed, calls originating nearby, but outside of the penitentiary grounds, were captured resulting in a number of improperly blocked calls. To resolve this issue, coverage was adjusted, leading to a decreasing number of intercepted calls. As the success of managed access is reliant on its coverage area, the signal strength of the managed access system cell tower requires routine observation and adjustment to ensure it provides adequate signal strength throughout, but not outside the designated coverage area. Since a cellular phone automatically connects to the strongest available signal from the subscriber providers' network, it is critical that a managed access system always presents the strongest signal to cell phones within the managed access system designated coverage area. Failure to actively monitor signal strength can result in a contraband cell phone connecting to a commercial tower outside the facility, bypassing the managed access system. Achieving optimal signal strength at MSP was not as simple as increasing or decreasing the managed access system signal power. Negotiations with at least one nearby cellular carrier was determined to be an important factor in maintaining proper coverage; MSP noted that they had to request that at least one carrier reduce downlink signal strength from a nearby cell tower.

To remain effective, coverage within the managed area must also be confirmed as the equipment ages and as the wireless environment around the facility changes over time. System effectiveness requires balance between wireless signal strength of the managed access system and nearby cellular carrier base station signals; the managed access signal must be configured so that that the managed access system signal is only strong enough to "capture" cell phones operating within its pre-defined operational area, and weak enough to ensure commercial

networks capture all phones operating legitimately in adjacent areas. It was noted that Global Tel Link conducts a drive test at least once per week around the perimeter of the facility (and the leased fields) to ensure that the managed access system does not exceed pre-designated coverage areas. It was noted that the MSP system drive test route covers approximately 36 linear miles. The MDOC estimated that after about six months of effort the number of nearby calls intercepted reached a steady state of roughly one call per month**.** Tecore noted that they developed a wireless coverage design for the MSP system, and then worked with each carrier to define/quantify signal coverage. It was noted that carriers were helpful during the design process; for example they suggested technical parameters such as required angles for managed access system antenna down-tilt. Spectrum access and conditions associated with managed access system design will vary significantly, and coverage parameters will be unique to each facility and, as previously noted, will require site-specific managed access network designs.

One example was provided by MSP personnel where a local farmer was tending his field near the facility and attempted to make a call while on his tractor. The farmer contacted MSP officials after receiving the automated recording generated by the system alerting the user of their illegal call attempt. This situation was remedied as MSP personnel reviewed his situation and included his number on the approved list. At the time of the site visit, MSP was in discussions with Tecore about the possibility of installing additional sub-sites (small cells) within the facility to improve system coverage within some buildings. These sub-systems would provide local signals strong enough to capture a cell phone in or near the building and then interact with the core switch. This would reduce the likelihood of bleed over by increasing the signal strength only within specific buildings.

Signal bleed over constitutes a serious consideration for potential managed access users, especially those located in more urban environments. Signal bleed over, as well as cellular carrier cooperation have implications for a widely acknowledged concern of managed access; interference with emergency 911 calls. The *Wireless Communications and Public Safety Act* of 1999 prohibits the use of any technology that can interfere with emergency 911 calls. The senior system administrator at MSP recalled that MSP and Tecore conducted tests of the call set up time for 911 calls through the managed access system. It was determined that a 911 call bypassing the managed access system took about 4.5 seconds to connect, compared to 7.0 seconds through the managed access system. Despite this slower time, this measurement is well-within the 10-20 second benchmark noted within the National Emergency Number Association (2006) call standards.

9-1-1 call management. A critical aspect of managed access system operation is the relationship between the managed access system, nearby commercial cellular system operators, and Public Safety Answering Points (PSAP). Authorized calls placed through managed access system are essentially placed once the user connects, or roams onto, the managed access system which processes the call for completion. Connection processes for service requests from authorized phones require network connections between the managed access system switch and cellular carrier mobile telephone networks and similarly, PSAP connections are required to successfully connect emergency 911 calls (see Figure 10.)

System deployment tasks include the establishment of support mechanisms to facilitate routing of emergency 911 calls. Typically, this involves a direct routing of calls between the managed access system core and a local 911 or PSAP call center to handle emergency calls passed to them from the managed access system. System interconnection and call completion

processes are influenced by local PSAP technical requirements and local landline telephone services associated with how the local the 911 network operates.

Tecore discussed how 911 calls are handled by the MSP system. It was noted that the MSP system routes 911 calls placed directly to the nearest PSAP. This is in contrast to other managed access implementations designed to simply pass emergency through cellular carriers for further processing and eventual call routing to a PSAP. It was noted that potential response issues will occur if the carrier is not provided information indicating that an emergency call originated within, or in the immediate vicinity of, the managed access system. As a result, cellular carriers may require emergency call routing directly to a 911 center/PSAP as a condition of a spectrum lease.

Technology upgrades by cellular carriers can significantly reduce system effectiveness. Managed access system coverage, and how it coexists with the surrounding cellular carrier environment, affects the ability of the system to terminate/block unauthorized calls and capture calls placed by legitimate device users operating devices in locations directly adjacent to the space controlled by the managed access system. The wireless environment is the primary interface between a user device and either a commercial network, or the managed access system network. Blocking calls associated with nearby legitimate cellular system users is considered to be interference by cellular carriers

Legal operation of a managed access system, using frequencies licensed to a network operator, must be carefully coordinated and authorized by both the carriers and the FCC to ensure legal access to carrier spectrum. MDOC indicated that there were several operational cellular carrier networks providing coverage in the Parchman area: AT&T, Verizon, C Spire, and either T-Mobile or Sprint. MDOC noted that commercial carriers had been cooperative, but the

processes associated with establishing managed access technology presented a new issue for commercial cellular network operators as well. When obtaining FCC authorization, spectrum lease arrangements are required for each carrier prior to operation of the system in their frequencies. As previously noted, the managed access system owner/operator needs to ensure that all wireless provider frequency bands in the area are covered by the managed access system. Tecore noted that the MSP project resulted in the first managed access spectrum lease agreement for Verizon. It was also noted that the MSP spectrum lease agreements do not involve recurring payments to the carriers although, in some cases, the cost of specific items such as carrier legal expenses required to prepare spectrum lease agreements were incurred.

A Tecore representative indicated that the company spent 18 months lobbying, negotiating with the FCC, and with interfacing with cellular system operator legal teams to define a regulatory solution/process suitable for managed access system deployment. Tecore indicated that these activities were well underway prior to the MSP system deployment. MDOC and Tecore emphasized the importance of carrier cooperation when establishing spectrum lease agreements. Global Tel Link is responsible for the ongoing operation of both the non-cellular inmate phone service, and the MSP managed access system. If a commercial service provider deploys a new cellular technology (e.g., 3G/4G LTE), Global Tel Link works with the managed access vendor to acquire necessary hardware and software upgrades required to ensure the managed access system continues to restrict network access via devices using the new technology.

This challenge requires collaboration and open communication with cellular carriers to manage network changes and carrier rollouts of new cellular device technology. Managed access system technology must be in sync with the commercial network to ensure that it can

capture devices made available to consumers. Advancements in cellular network technology occur over time, and then are activated in a very short timeframe. Even if managed access users are informed in advance of planned carrier updates, there are a number of potential negative consequences for managed access systems as a result of commercial network changes as a carrier makes an upgraded service or capability available within the market surrounding the managed access system.

This was the case for MSP when AT&T activated 3G technology in the Parchman area. The managed access system at MSP was not yet capable of capturing 3G cell phones. As a result, any call attempts from a contraband cell phone using 3G went directly to the commercial carrier. Anecdotal information also suggests this AT&T 3G rollout coincided with a significant reduction in calls captured by the system. As the managed access system hardware and software were updated to be compatible with 3G technology, the number of denied calls appeared to elevate and return to pre-3G levels. It should be reinforced that this relationship is speculative and assumes that contraband cell phones were 3G capable. Data to test this relationship were unavailable.

Network operators grow their networks and update technology over time, and these changes will impact the effectiveness of a managed access system. Timely notification to managed access operators about change in nearby commercial networks is paramount. MDOC noted that subsequent to MSP system deployment AT&T activated 3G services in the Parchman area, without advance notification to MDOC. It was several months before MDOC realized that the managed access system needed to be upgraded to intercept 3G calls. It was also noted that carriers were supportive in regard to notifications, but the notification process was not routine for them; therefore notifications were inconsistent. A managed access system operator needs to

receive notifications well in advance of carrier changes so that the impact to the managed access system can be assessed, allowing time for corresponding managed access system hardware/software upgrades, and/or coverage changes in response to the changing wireless environment. Global Tel Link and Tecore indicated that carrier sublease agreements include notification clauses but they do not include required enforcement mechanisms.

Managed access infrastructure needs to be hardened. The MSP system experienced occasional power issues such as brown-outs and outages that were beyond the control of MDOC or managed access system vendors. A variety of additional uncontrollable factors affected system performance. For example inclement weather causing high winds can change the orientation of the antenna system. MDOC does some level of troubleshooting to identify when and where problems occur, and the attitude of the MDOC and their commercial partners is that all technical issues were solvable. Tecore indicated that the system was continually being improved, and that the issues described were occasional problems.

Inmates may attempt to sabotage the system infrastructure. A final challenge that was observed at MSP was the ever-present need to harden system infrastructure against vandalism. There were two specific incidents in which inmates at MSP attempted to sabotage the managed access infrastructure. One attempt involved inmates cutting exposed cables running from underneath an equipment enclosure while the other involved an inmate on agricultural assignment running a field tractor into an equipment enclosure. Follow-up investigations into these incidents revealed a directed attempt to sabotage the system. To protect against such incidents, MSP personnel buried all cable and erected fencing around exposed system infrastructure. These hardening efforts constituted unplanned financial costs incurred by MSP.

Practices and Lessons Learned.

For organizations seeking to implement a managed access system, a number of lessons were learned from MSP's experience. These lessons learned are provided to inform both practitioners and vendors of mechanisms to enhance the effectiveness of managed access. A summary of these lessons learned and the context within which they can be applied are provided in Table 3.

Table 3. Summary of Operational Lessons Learned and Context for their Application

Lesson Learned	Context of Application
1. Advocate for amendments to existing legislation governing contraband cell phones	• Legislation was amended to close loopholes in the law Rather than an inmate having possession of a complete cell phone, legislation prohibits possession of any part of a cell phone (i.e. battery, SIM card, etc.)
2. Establish cooperative partnerships with cellular carriers	• Effective reach of managed access is greatly enhanced with additional carrier support Ability to prove a cell phone is operating within correctional facility to allow a carrier to permanently disable the device
3. Cross-reference captured phone call information with existing pre-approved list of inmate landline numbers	• Managed access captures the destination phone number of illegal cellular call attempts and makes it possible to cross reference these destination numbers with existing pre-approved inmates contact numbers for landline use This cross reference allows correctional personnel to identify the inmate likely possessing a contraband cell phone
4. Managed access provides a layered approach for counter-measures beyond traditional search capabilities	• Deterrence resulting from legal sanction and inconsistencies with physical searches yield limited impact on combating contraband phones from reaching the hands of inmates Managed access provides a significant counter-measure that specifically targets cell phones that have been successfully smuggled into the facility

5. Increase in the number of monitored inmate conversations via landlines	• Decreases in the success rate of contraband cell phones leads to an increase of landline use by inmates This increase allows for more conversations to be monitored for investigative and evidentiary purposes
6. General deterrent of managed access to impact contraband cell phone market value	• Anecdotal evidence suggests managed access impacts the value of contraband cell phones within the facility If a phone is perceived to work only once or not at all, inmates will likely not invest in the device
7. Creation of a contraband cell phone unit within MSP	• By formally sanctioning and physically housing these habitual cell phone inmates, they can be more closely monitored as well as removed from the general population of inmates that may rely on them for access to a cell phone

Amendments to existing legislation governing contraband cell phones. At the time managed access was installed in MSP, the state's criminal code guiding inmate possession of contraband was limited to traditional items such as weapons and drugs. In order to establish a legal precedent for inmates not to be in possession of a cell phone, as well as serve as a sanction-based deterrent, the Mississippi legislature amended the criminal code to include "cell phone" in the language. However, the legislation could be circumvented by parting out cell phone devices to ensure that one could not be found in possession of a fully-assembled cellular device. To remedy this issue, MSP officials solicited further assistance from the state legislature to amend the criminal code again to control for this technicality. In early 2012 the state legislation amended the criminal code to include the language "unauthorized electronic device" as well explicitly identifying "cell phone." This criminal code also now specifies that possession of a cell phone within a correctional facility is a felony with a three to fifteen year sentence. The

revised and now current criminal code guiding contraband within MSP is as follows (last revised in early 2012):

> "§ 47-5-193: Prohibitions generally: It is unlawful for any officer or employee of the department, of any county sheriff's department, of any private correctional facility in this state in which offenders are confined or for any other person or offender to possess, furnish, attempt to furnish, or assist in furnishing to any offender confined in this state any weapon, deadly weapon, unauthorized electronic device, cell phone or contraband item. It is unlawful for any person or offender to take, attempt to take, or assist in taking any weapon, deadly weapon, unauthorized electronic device, cell phone or contraband item on property belonging to the department which is occupied or used by offenders, except as authorized by law" (State of Mississippi, 2012).

This lesson learned may seem to be a daunting task. However, based on communications with MSP personnel, this logistical and political process was streamlined with Global Tel Link, Tecore, legislators, and the various MDOC supervisors working together with minimal obstruction in order to implement the entire operation smoothly. MDOC noted that the state legislature had "consistently shaped laws and policy to meet our needs." The linear nature of the chain of command from the state-level through to the managed access supervisors appeared to greatly assist this effort. Perhaps even more important was the perception of MDOC personnel that the state administration was "wide open to legitimate change, they want to be hands-on and proactive in solving this problem." The Commissioner of MDOC in particular was credited for taking a proactive leadership role in streamlining the technology's implementation.

Establish cooperative partnerships with cellular carriers. In the same vein, it was also found that cooperative partnerships between cellular commercial carriers, MSP, and MDOC officials have the potential to enhance the impact of managed access. Retrieving cell phone hardware or the entire device is the ultimate goal of contraband cell phone interdiction efforts but is not always possible. Through the detection of cell phone transmissions emanating from specific devices it is possible to permanently disable a cell phone on a commercial network. Personnel

at MSP and MDOC worked in collaboration with carriers to establish a process and set of evidentiary criteria to prove the use of a particular cell phone device from within MSP. With this evidence, MDOC and commercial carriers can request a court order to permanently disable the voice, text, and data transmission capability of a phone and/or de-authorize Subscriber Information Module (SIM) cards This process described is very analogous to the "kill switch" approach under consideration in ongoing FCC proceedings. .

Data on the frequency with which cell phone devices were permanently disabled are not available. Discussions with key informants and affiliated stakeholders suggested that while a cell phone could be disabled, the frequency in which this process is executed is rare. Additionally, it must be noted that contraband cell phones can still produce harms without a transmission capability. Managed access or similar technologies should not be relied upon as a substitute for physical device confiscations.

Cross-reference captured phone call information with existing pre-approved list of inmate landline numbers. In order for inmates to use the designated landline telephone system within MSP, they must first provide for approval, a list of up to ten telephone phone numbers they wish to call at any given time. MDOC personnel vet and if approved they are added to the inmates' list of contacts contained in the landline phone system. Each inmate has a unique code they must enter when making a landline call. Once this unique code is entered, the inmate can only call contact numbers processed into the system. To ascertain if a particular cell phone was being operating from within MSP, transmissions intercepted by the managed access system are compared to inmates' pre-approved landline call lists

If a call attempt is captured by the managed access system is placed to a number that is also in an inmate's pre-approved contact list, it is assumed that the inmate has the contraband phone

in their possession or has information pertaining to the phone. Through this method, MDOC estimates approximately 90% of captured transmissions can be linked to MSP inmates. Given the quantity of data produced from the managed access system, it was noted that personnel resources limit use of this investigative method for day-to-day operations.

Managed access provides a layered approach for counter-measures beyond traditional search capabilities. The impact of managed access at MSP is perhaps best viewed through a layered approach. In this conceptual model, managed access provides two additional layers of safeguarding against cell phone use beyond traditional search protocols used in correctional facilities. Search activities involve sanction-based legal deterrents; physical pat-downs, metal detectors, dogs, and random search teams of inmate housing. With the exception of random cell searches, these attempts to combat contraband target offenders prior to a cell phone reaching the interior housing unit of a facility. A managed access system adds: 1) the capability to block cell phone transmissions originating or terminating within the facility, and 2) the potential to disable the transmission capability of a contraband device through collaboration with network carriers. It must be emphasized that sanctions and physical security are the foundation of counter-contraband efforts. Managed access technology should not be interpreted as an appropriate substitute for these efforts. Managed access is a supplemental technology to contraband and specific only to cell phones. This layered approach is illustrated in Figure 13.

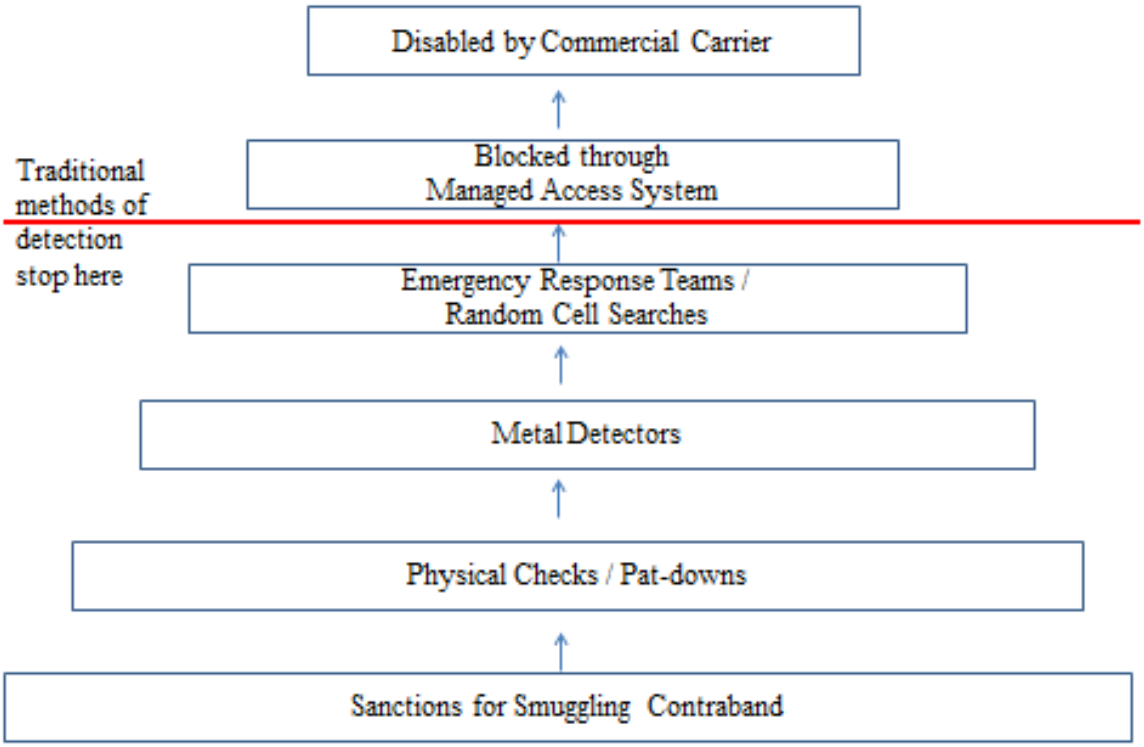


Figure 13. Layered Approach to Combat Contraband Cell Phones

Increase in the number of monitored inmate conversations via landlines. MDOC representatives believed the number of cell phones confiscated decreased as a result of the managed access system installation and associated revenue incurred from the inmate phone system. This suggests that installation of a managed access system increased inmate use of landline telephones to make calls. Aside from generating additional revenue for both the state department of corrections as well as the vendor, this increase in call activity via landline phones also leads to an increase in the number of conversations that are recorded and reviewed. Though MDOC officials could not determine the proportion of landline calls were later tied to criminal behavior, it seems apparent that by virtue of the increased land-line call volume there would be a

proportional increase in the number of inmate communications with evidentiary or investigatory value.

General deterrent of managed access to impact contraband cell phone market value. In addition to the anecdotal increases in landline calls, MSP personnel indicated that inmates have begun to recognize the effect of the system on the contraband marketplace within the facility. It is believed that as cell phone transmissions are blocked, inmates are less willing to spend hundreds of dollars to obtain a cell phone that cannot complete call or text transmissions.

Creation of a contraband cell phone unit within MSP. Lastly, one of the more interesting lessons learned at MSP was their creation of a special "contraband cell phone unit." This unit was a stand-alone physical housing area for habitual cell phone users. As with general crime, it is believed the majority of cell phone use within prison results from a minority of the inmates engaged in the use of contraband cell phones. By formally sanctioning and physically housing these habitual cell phone inmates, they can be more closely monitored as well as removed from the general population of inmates that may rely on them for access to a cell phone.

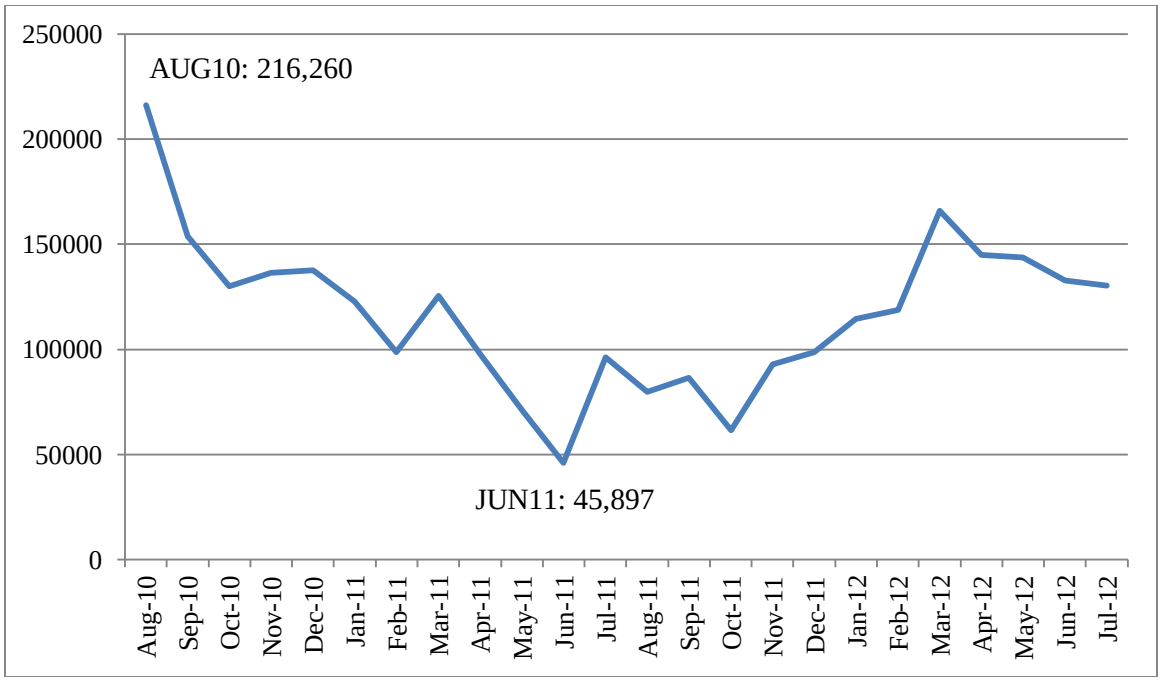
Inmates placed in this special unit lose privileges. Officials from MSP emphasized that correctional staff overseeing this unit were "hand-picked to avoid personnel who might have provided them with phones." The MSP officials also explained that this approach is good in theory, but in practice it is difficult as the number of offenders that have repeat cell phone offenses is simply too large to assigning prisoners to the special cell phone unit. It appears this special unit is more of a temporary housing unit than a long-term solution to help remedy the problem. At the time of the research team site visit, MSP officials were discussing the need to identify what appropriate benchmarks would be for assigning someone to this special unit, such

as three or four violations before being admitted. At the time of this report writing, no determinations had been made with respect to such benchmarks.

Contraband Cell Phone Activity

Total Monthly Call Attempts from August 2010 Implementation through July 2012. On average, 116,754 call attempts (SD = 36,848.07) were made each month, with a median of 120,800 call attempts. The maximum number of call attempts detected occurred immediately after implementation in August 2010. Gradual decreases in detected call attempts were observed after implementation, with the managed access system detecting 45,897 call attempts in June 2011. The number of monthly detected call attempts decreased by 79% from August 2010 to June 2011.

Though it cannot be determined for certain, this dramatic decrease in call attempts captured by the managed access system is believed to have resulted from the rollout of 3G service from AT&T. Beginning in July 2011, the number of detected call attempts began to increase dramatically but did not return to the levels of detection observed in the first few months after implementation. The number of detected call attempts nearly doubled from June 2011 to July 2012. Acknowledging with the curvilinear U-shaped distribution of these data, there are linear and exponential decreases in the number of detected call attempts from August 2010 through July 2012. Figure 14 illustrates the distribution of these monthly call attempts.

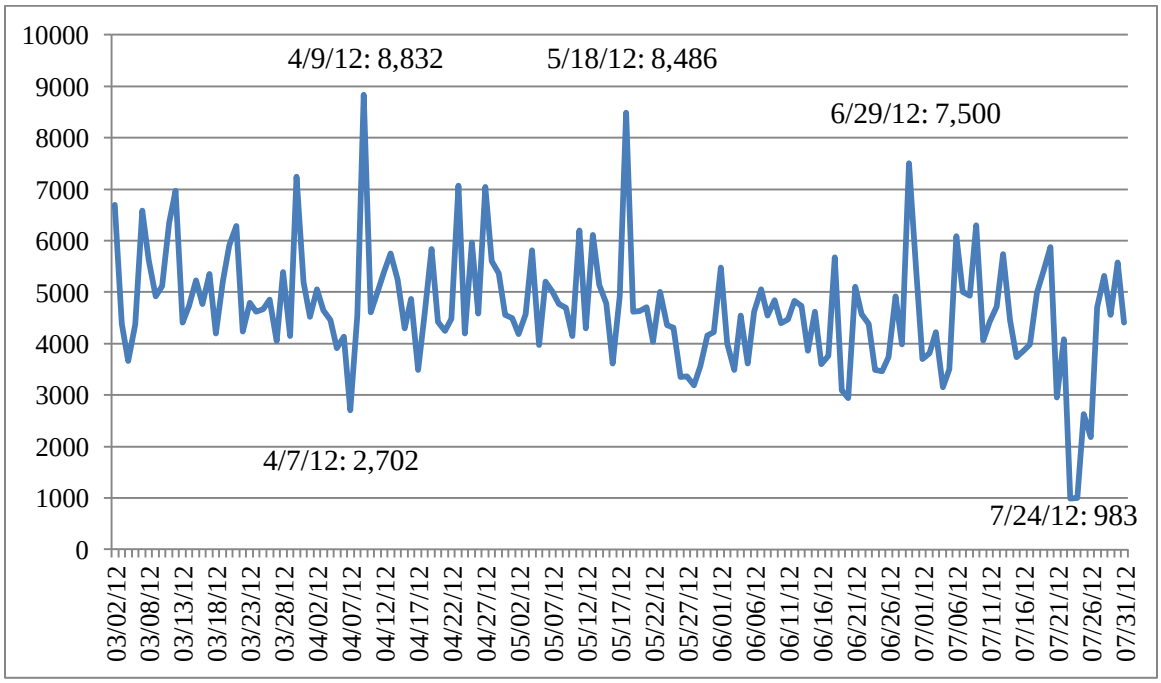


Source: Mississippi Department of Corrections, Managed Access System Data (Gleaned from Mississippi Department of Corrections, 2013)

Figure 13. Monthly Total Call Attempts Detected by MAS

Daily Call Attempt Volume March – July 2012. A total of 706,387 call attempts were detected from March 2012 through July 2012. It is important to note that this time frame is a period of gradual decline in monthly total call attempts after a peak in March 2012 (see Figure 14). The average number of calls per day is 4,678 (SD = 1,126.33), with a median value of 4,584 call attempts. The number of call attempts detected varied widely; ranging in value from 983 attempts on July 24th to 8,832 on April 9th (see Figure 15). Once again, there are linear and exponential decreases in the number of detected call attempts over time.

Examining some of the milestone or anchor dates within the available timeframe, the frequency of occurrence for connection attempts detected was substantially higher than average for Mother's Day (totaling to 6,110). This can be compared relative to the below average frequency of connection attempts detected for Easter Sunday (4,541), Father's Day (3,758), and Memorial Day (3,191).



Source: Mississippi Department of Corrections, Managed Access System Data

Figure 14. Daily Total Call Attempts Detected by MAS: Five Month Extract

Overview of Cellular Connection Measures Captured by Managed Access. The average cell phone device transmission detected by the system was a call (rather than a SMS text) using a Code Division Multiple Access (CDMA) radio system. Detected call attempts tended to occur between the hours of 8:00 a.m. and midnight, with noon to 3:59 p.m. representing the time frame of most frequent detected call attempts. Comparing the cellular frequency band, mobile network provider code by call attempt type reveals some baseline characteristics of detected call attempts. Detected call attempts show that voice calls are more likely to occur on CDMA radio systems, while SMS texts are more evenly distributed between GSM and CDMA technologies. Mobile network provider codes were also relatively similar. Unknown/unlisted call attempts detected by the system appeared to come from calls. A higher proportion of AT&T services were being used for SMS texts rather than calls. Tables 4-7 present counts for captured cellular call and text call attempts across different technology, cellular radio frequency, network carrier, and time of day.

It is important to contextualize the 40% of unknown/unlisted Mobile Network Codes observed in the data. The daily call attempt data provided by MDOC included International Mobile Subscriber Identity (IMSI) information captured by the managed access system, in standard format, from which the Mobile Network Code associated with the cellular service provider network could be derived. Unidentifiable or obsolete Mobile Network Codes were observed in the data (e.g., 006, 232, and 726) that could not be linked to a cellular service provider. The status of these MNCs remains unresolved. It is unclear if these codes are the result of device misconfiguration or some other use.

Table 4. Overview of Call Attempts by Type, Channel Access, and Mobile Network Code

	Frequency of Occurrence	Percent
Attempt Type		
Call	645,722	91%
SMS	60,665	9%
Channel Access		
CDMA	508,400	72%
GSM	197,987	28%
Mobile Network Code		
Verizon Wireless	220,633	31%
AT&T	171,034	24%
T-Mobile	27,292	4%
Mid-Tex Cellular	3,287	1%
Airadigm	115	<1%
Cincinnati Bell	1	<1%
Unknown/Unlisted	284,025	40%

Source: Mississippi Department of Corrections, Managed Access System Data

Table 5. Frequency of Call Attempt by Time of Day

Time of Day	Frequency	Percent
12:00-3:59 AM	26,616	4%
4:00-7:59 AM	80,704	11%
8:00-11:59 AM	140,146	20%

12:00-3:59 PM	179,098	25%
4:00-7:59 PM	155,212	22%
8:00-12:00 PM	124,611	18%

Source: Mississippi Department of Corrections, Managed Access System Data

Table 6. Channel Access by Call Attempt Type

	Call Attempt Type	
Channel Access	Call	SMS
CDMA	74%	47%
GSM	26%	53%

Source: Mississippi Department of Corrections, Managed Access System Data

Table 7. Mobile Network Code by Call Attempt Type

	Call Attempt Type	
Mobile Network Code	Call	SMS
Verizon Wireless	31%	37%
AT&T	22%	50%
T-Mobile	4%	3%
Mid-Tex Cellular	<1%	<1%
Airadigm	<1%	<1%
Cincinnati Bell	<1%	---
Unknown/Unlisted	43%	10%

Source: Mississippi Department of Corrections, Managed Access System Data

Connection Attempt Volume by Unique Cell Phones. All of the detected connection attempts were generated from 3,654 unique cell phone devices. These attempts equate to an average of 193.32 attempts per cell phone device (SD = 855.23). A median value of 11 connection attempts and mode of one call attempt was observed. Distribution of call attempts by cell phone device was not constant. Table 8 presents the frequency of occurrence of call attempts by unique device.

Table 8. Frequency of Occurrence Call Attempts by Unique Device

	Frequency Occurrence (%) of Total Call Attempts	Frequency Occurrence (%) of Cell Phones
Phone Used One Time	539 (<1%)	539 (15%)
Phone Used One to Two Times	1,151 (<1%)	845 (23%)

Phone Used One to Three Times	1,775 (<1%)	1,053 (29%)
Phone Used One to Four Times	2,571 (<1%)	1,252 (34%)
Phone Used One to Five Times	3,326 (<1%)	1,403 (38%)
Phone Used One to 10 Times	6,489 (1%)	1,811 (50%)
Phone Used 100+ Times	661,213 (94%)	771 (21%)
Phone Used 1,000+ Times	464,510 (66%)	153 (4%)
Phone Used 10,000+ Times	92,884 (13%)	7 (<1%)

Source: Mississippi Department of Corrections, Managed Access System Data

Of the 3,654 cell phone devices used, 15 percent (n=539) were used for one call attempt with no subsequent transmissions detected by the managed access system. The remaining 85 percent (n=3,200) of cell phone devices detected by the system were used more than one time. Most of the call attempts detected came from a small proportion of devices that were used frequently. Twenty-one percent of the cell phone devices used to make call attempts were responsible for 94 percent of the overall call attempts. Sixty-six percent of the total call attempts detected came from 153 cell phones devices, which were used more than 1,000 times. Seven devices were responsible for generating 10,000 or more call attempts. Preliminary analysis of one of the most used phones indicated series of stops and starts, with "blasts" of calls/texts within short timeframes to customer service lines and functional dial strings. However, note that this analysis was performed on a limited set of data that may or may not be representative, and we cannot derive any conclusion about the behavior of the phone or its user.

Average Cell Phone Lifespan. The data allowed for a determination of a device's lifespan. The difference in days between the date in which a device transmission was first captured by the system and the date in which the device transmission was last captured can be interpreted as how long a device had been used and detected by the managed access system. This analysis begins to dissect the aggregate trends and explore transmission patterns.

The average lifespan for the top seven devices used 10,000 or more times were estimated (see Table 9). As a reminder, the period of observation is March 2012 through July 2012 which

totals to 151 days. Average lifespan of these top seven phone devices in the observation period is 96 days (SD = 43.25), with median and mode values of 86 days.

Table 9. Cell Phone Lifespan by Unique Device

Device	Total Number of Transmissions	Lifespan (in Days)
A*	20,037	86
B*	15,074	129
C*	13,153	150
D	12,029	65
E	11,124	26
F*	11,053	130
G*	10,414	86
Mean (SD)	13,269 (3373.37)	96 (43.25)

The lifespan analyses allow for calculation of how long these devices were in use within the observation period. Asterisked devices in Table 9 identify devices with captured transmissions at the start or the end of the observation period. One of these five devices (Device C) was active at the start of this observation period, which means that this device was likely in use ***before*** March 2012. The remaining four devices (Devices A, B, F, and G) were active at the end of the observation period, suggesting these devices were likely in use ***after*** July 2012. In combination, these lifespans should be interpreted as very conservative estimates.

These analyses provide preliminary evidence that devices were both used at a relatively constant rate across the 151 day observation period to become one of the top devices used 10,000 or more times (see Devices B, C, and F) as well as a highly variable or non-constant rate (see Devices D and E) to amass a large number of transmissions. Unfortunately, no data was available to determine if device lifespans with clear first and last transmission dates (i.e., Devices D and E) is a function of devices being confiscated, destroyed, or simply lacking a battery charge. It is also possible that while these devices may no longer be detected by the managed access system, they still may be used for other purposes (e.g., audio and video recording).

Call Attempt Volume by Destination Number. A total of 30,835 unique destination numbers were dialed within the five month data sample. These numbers contain a mixture of functional strings (e.g., XXX-XXX-XXXX, 1-XXX-XXX-XXXX, or XXX-XXXX formats), SMS text shortcuts, and unusable numbers (.e.g. *#72). The average number of times a destination number was dialed was 23 times (SD = 1,656.92), but this estimate is extremely skewed with a few numbers being dialed thousands of times. The median number of times a number was dialed is twice, with a mode of one. As indicated by Table 10, most of the destination numbers used were repeatedly dialed less than 10 times.

Table 10. Frequency of Occurrence of Call Attempts by Destination Number

	Frequency of Occurrence (%) of Numbers Dialed
Number Dialed One Time	13,058 (42%)
Number Dialed One to Two Times	18,193 (59%)
Number Dialed One to Three Times	20,833 (67%)
Number Dialed One to Four Times	22,607 (73%)
Number Dialed One to Five Times	23,820 (77%)
Number Dialed One to 10 Times	26,827 (87%)
Number Dialed 100+ Times	360 (1%)
Number Dialed 1,000+ Times	27 (<1%)
Number Dialed 10,000+ Times	7 (<1%)

Source: Mississippi Department of Corrections, Managed Access System Data

Call Attempt Volume by Top Destination Numbers. Table 11 presents the attempt frequency of occurrence of each number and a brief description of the number dialed for top 10 call attempts via cellular call. The most commonly attempted numbers called include a mix of services. These include a shortcut connection to wireless Internet access, a shortcut or 1-800 number to cellular provider customer service line, a variety of free, anonymous voicemail accounts, a chat line, pre-paid credit cards, and a 24/7 free service line where adults read children's books and the recording of stories is available on a constant loop.

A #777 dial string was used to provide a "tethered" data connection using 3G services. The #777 is used for Global System for Mobile Communications (GSM; affiliated with Verizon,

Alltel, and Sprint) and an analogous dial string for CDMA is #99xxxxx (affiliated with AT&T, Cingular, and T-Mobile). The #777 number was often (but not always) used in conjunction with a password that typically was the ten-digit cellular number associated with the phone service. It is interesting that the CDMA #99xxx number does not appear on this list as well. All of the Seattle, WA numbers are for voicemail services. This service provides users with free unique personal number that callers leave messages on and can listen to using the same number.

Table 12 presents the attempt frequency of occurrence of each number and a brief description of the number dialed for top 10 SMS text attempts. Texted phone numbers are far less concentrated than phone numbers called. For the most part, texts are being delivered to private numbers. During an open source Internet search of these numbers, many were openly listed on social networking profiles of individuals or electronic wanted ads of individuals or businesses. The most commonly texted number (1111340002) is associated with automated "robot" dialing. Based on open-source research, this specific number appears to be associated with a debt collection service. Why this number would be the recipient of inmate text messages is unknown.

Table 11.Top 10 Destination Numbers Called

	Frequency Occurrence (%) of Total Call Attempts	Description
#777	280,911 (44%)	Connect to wireless Internet
611	63,995 (10%)	Access customer service
(206) 208-XXXX	24,449 (4%)	Inactive voicemail account, Seattle (WA), International Telcom, Ltd.
(509) 676-XXXX	21,123 (3%)	1 to 1 chat line, Walla Walla (WA), Telewise
1-800-331-XXXX	11,995 (2%)	AT&T customer service
(206) 208-XXXX	11,702 (2%)	Inactive voicemail account, Seattle (WA), International Telcom, Ltd.

1-800-473-XXXX	10,926 (2%)	Green Dot MoneyPak customer service
1-800-473-XXXXX	9,445 (1%)	Misdial of Green Dot MoneyPak line (+1 digit)
(206) 208-XXXX	6,356 (1%)	Inactive laser voicemail account, Seattle (WA), International Telcom, Ltd.
(601) 482-XXXX	3,875 (1%)	Public Library Story Line, Meridian (MS), Bellsouth Telecomm Inc.

Source: Mississippi Department of Corrections, Managed Access System Data

Table 12.Top 10 Destination Numbers Texted

	Frequency of Occurrence (%) of Total SMS Attempts	Description
1111340002	1,401 (2%)	Access Integrated Services Digital Network
(662) 267-XXXX	781 (1%)	Private number, Batesville (MS), Sprint
(314) 225-XXXX	642 (1%)	Private number, Ladue (MO), New Cingular Wireless
(562) 618-XXXX	550 (1%)	Private number, Compton (CA), New Cingular Wireless
(601) 613-XXXX	348 (1%)	Private number, Jackson (MS), New Cingular Wireless
1-601-502-XXXX	328 (<1%)	Private number, Jackson (MS), Bellsouth Telecomm
(601) 529-XXXX	273 (<1%)	Private number, Vicksburg (MS), New Cingular Wireless
(901) 483-XXXX	270 (<1%)	Private number, Memphis (TN), Cellco Partnership/Verizon Wireless
(407) 403-XXXX	269 (<1%)	Private number, Orlando (FL), New Cingular Wireless
(318) 837-XXXX	265 (<1%)	Private number, Wisner (LA), New Cingular Wireless

Source: Mississippi Department of Corrections, Managed Access System Data
Note: These numbers represent the exact format in which numbers were dialed and captured.

Case Flow of Call Attempts: January to April 2012. Figure 15 provides an illustration of case flow processing of cell phone confiscations at MSP and among the remainder of MDOC's facilities. The overall trends identify two salient concerns for correctional administrators. First

is the confiscation-sanction gap. The number of cell phones confiscated exceeds the number of violation reports and prosecutions. Second is the gap between the number of cell phone devices available for use and the proportion that are confiscated. Noting that the data on the number of unique devices is only available for the months of March and April and likely underestimates the actual number of unique devices, it appears that only a small proportion of available devices are confiscated.

A few points of comparison can be made between MSP and all of the remainder of MDOC's facilities. MSP appears to have a slightly higher percentage of cell phones devices discovered on person relative to all other MDOC facilities. Contrary to this higher percentage of inmate possession of contraband cell phone devices, MSP has a lower proportion of cases moving forward with prosecution as compared to other MDOC facilities. It is also worthy to note that MSP appears to generate more rule violation reports and forward more cases to the local District Attorney net of the total number of cell phones confiscated. Since these de-identified data do not allow for determinations of individual case decisions at these phases, case flow trends for rule violation reports and forwarded cases must be interpreted with caution.

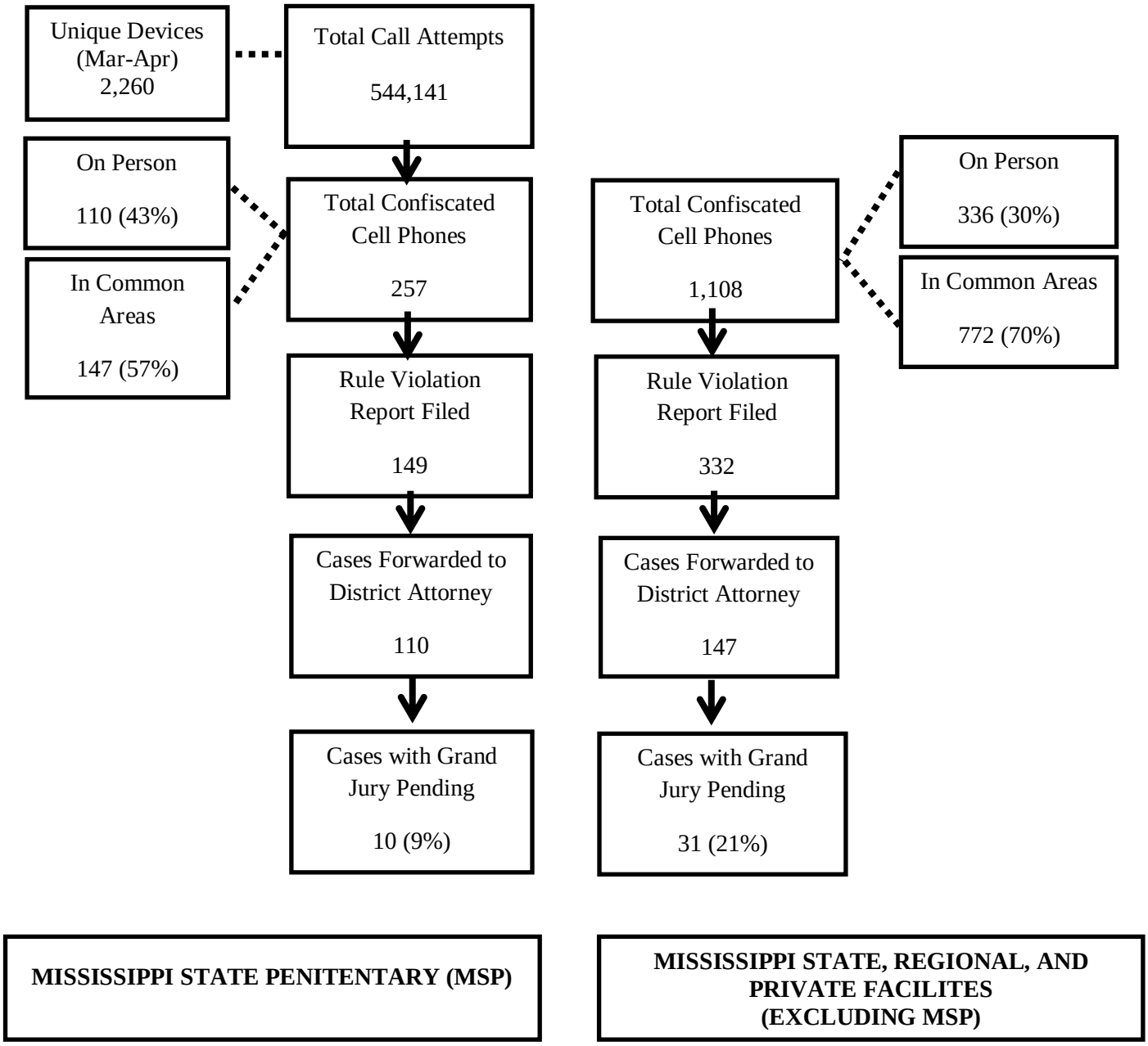


Figure 15. Case Flow Trends: January to April 2012

Discussion and Conclusions

The present research provides four unique insights. First, the contraband cell phone problem is perhaps more significant than imagined. One of the themes discussed throughout the site visit was the increase of inmate access to contraband cell phones from within correctional facilities. Based on the managed access system data, the median number of daily call attempts within MSP was 4,584. This can be extrapolated to estimate that 1,673,160 illegal cellular call attempts will occur in MSP alone in a single year.

Generally, the contraband cell phone problem has been illustrated to date by using the number of devices seized. The measurement of call attempts generated by the managed access system provides a useful alternative to understand the extent of contraband cell phone use. Moreover, call attempt data provides insight on the gap between estimated call attempts from unique cell phone devices and seized devices. While MSP is a relatively unique facility given its size, location, and history, the observed call attempt estimates may be similar across facilities with comparable rates of contraband cell phone confiscation within Mississippi and across other states.

Second, the managed access system at MSP does appear to work. That is, the system is able to detect and inhibit transmissions from cell phone devices within MSP. The system handles a large volume of call and text attempts and captures a variety of information that can be cross-referenced to facilitate subsequent administrative or investigative decision points. At the same time the extent to which managed access works is contingent on a number of system, personnel, and interagency cooperation and communication factors discussed throughout this report. If these elements are not actively managed, the ability to detect and inhibit cell phone transmissions can be dramatically reduced or lost altogether.

Relatedly, there is evidence to question the operational theory of managed access and what the system can provide correctional administrators. Perhaps the weakest proposition affiliated with managed access is the notion that such systems render cell phones as obsolete or useless. Managed access does not directly disable a cell phone by terminating voice, text, and data transmission capabilities and/or de-authorizing a SIM card. Instead, data generated from the managed access system is shared with commercial carriers to facilitate a court order to disable a cell phone. While feasible, this process is rarely pursued. Managed access does not ensure that once a cell phone is detected by the system the device is no longer used. The overwhelming majority (85%) of cell phones detected by the system were used more than one time and a small proportion of cell phones detected by the system attempted to transmit hundreds of call and/or text attempts. Managed access also does not appear to produce higher rates of cell phone confiscation relative to all other MDOC facilities. While call or text transmissions may be blocked by managed access, these devices do not seem to be discarded and subsequently confiscated by correctional personnel.

Third, managed access technology has operational shortcomings. As discussed, the technology requires active management on behalf of the adopting organization (see Tables 2 and 3 for a summary). Relatedly, the effect of the technology on the repeated use of cellular devices is not entirely clear. As noted, there were a small proportion of cell phone devices that were continuously used across a number of months to attempt calls and/or texts. These devices were responsible for a large portion of the total transmissions detected by the managed access system. These findings call into question how data generated from the system are automated and analyzed to produce actionable intelligence. The sheer volume of data produced as well as the mix of functional, misdialed, or erroneous dial strings may make it difficult to cross-reference

the destination number of contraband call attempts and inmates' pre-approved landline contact lists. The possibility does exist that this process could be automated to reduce the labor-intensive nature of cross-referencing numbers. However, such a process is likely to include specialized analytical skills, tools, and programming capabilities for translational comparison that may not be available to some corrections agencies.

Lastly, and perhaps most intriguing, the present research has shed light on unauthorized contraband cell phone activity. As specifically illustrated in Tables 11 and 12, a wide-range of communications are being attempted with contraband phones. Though the present research falls dramatically short of determining social support versus criminal coordination with these transmission attempts, it lends some empirical support for the use of contraband cell phones to fulfill an array of user needs which may not differ from cell phone users in the community (see Aoki & Downes, 2003). This is certainly not to say criminal activity does not occur through these contraband phones; it is almost certain that it does as well. However, these attempted calls or texts are not prospectively identifiable in the managed access system data.

The question is whether or not managed access is worth the financial investment. The answer to this question involves a myriad of complex issues and decisions. Managed access does capture a large quantity of cellular transmissions, but it is impossible to determine the rate with which attempted calls or texts successfully elude detection by the system. Even if a hypothetical rate of successful transmission detection was only 40 percent, that 40 percent would provide a substantial value-added effect to combating contraband cell phones problem relative to existing countermeasures. Thus, the decision comes down to this benefit versus the cost of installing and maintaining a managed access system.

Cost estimates are difficult to obtain for proprietary reasons. However, based on open-source information a significant monetary investment is required. Baltimore City Detention Center (BCDC) in Baltimore, Maryland implemented a managed access system. The technology will be deployed over 700,000 square feet of targeted area within the facility and utilize a full scope of commercial wireless spectrum (Tecore Networks, 2014). System costs are estimated at $5.4 million (Washington Post, 2014).

Limitations

This research has a number of limitations and rests upon a variety of assumptions. To begin with, this study is exploratory in nature and sought to establish a foundation upon which future research on managed access can be conducted and practitioner decisions regarding the procurement and implementation of managed access technology could be based. Given the infancy of managed access technology and the sparsely available operational systems that can be evaluated, relatively limited information was available to guide the present research. Despite the limitations to be addressed here, the research has yielded a number of insightful and intriguing findings that will impact future practice and research.

Data limitations significantly hindered the study. Due to a number of unforeseen personnel changes within MSP and proprietary system concerns from the vendor which also owned the landline inmate calling system, an assortment of data was simply not available to the research team. Data was only available post-managed access system installation. Ideally the research team would have been able to collaborate with MDOC personnel to identify appropriate pre-installation measures related to contraband cell phone use at MSP. These metrics could have included inmate contraband and discipline reports, correctional staff discipline reports for smuggling cell phones, the type of cell phones confiscated, and survey and interview data from

inmates and staff at MSP regarding the prevalence of contraband cell phones, the catalysts behind inmates' use of these phones, and inmates awareness of MSP efforts to combat the use of cell phones. Without pre-implementation measures, it is difficult to determine the effect of managed access technology on correctional operations.

Data utilized by the present research is also limited in scope with regard to the temporal period examined. The managed access system became operational at MSP in August 2010, yet the available data utilized for secondary analysis only captured a five-month snapshot of a post-deployment period. The justification for utilizing this March – July 2012 time frame was 1) this time period is believed to be the most operationally-efficient of the system and 2) the tedious time-intensive process to clean and organize the data for analysis was significant. In addition, when the data from this time period is compared across previous post-deployment months (i.e., August 2010 to February 2012) there were no statistically significant differences in mean transmissions detected by the system. As such, the five-month snapshot data does not appear to be unrepresentative of broader monthly trends.

This research is unable to identify and distinguish whether attempted calls or texts captured by the managed access system are coming directly from inmates who are actively using contraband cell phones. The fundamental operational assumption of this technology – non-approved phone numbers that are intercepted and blocked are illegally made by inmates with contraband cell phones – could not be empirically examined. MDOC provided anecdotal estimates that 90 percent of attempted transmissions can be cross-referenced to pre-approved landline call lists and linked to MSP inmates, which increases the validity of managed access system data. At the same time, this estimate acknowledges measurement error that may be associated with the management of authorization lists and coverage leakage issues. There is also

some evidence to suggest that unauthorized call or text attempts may be made by a passive, automated process affiliated with cellular device hardware or software than user dialing. For example, earlier it was noted that #777 is a number dialed by a device to obtain data service from a wireless network. It is unclear if this number is manually dialed by a user seeking service or if the call attempts are from a cellular device programmed to continuously dial this number in search of service. It is possible that these call attempts are part of automated managed access coverage testing. Additionally, it is not clear if detected transmissions originate from users that have multiple cellular devices or from a user who possesses one Subscriber Identity Module (SIM) card that is shared among others with compatible cellular devices. The findings should be interpreted with these limitations in mind.

This assessment does not include information pertaining to costs. Any attempt to quantify costs related to system build out, maintenance, or ancillary expenses (i.e., personnel and training) was deemed to be invalid and unreliable. Cost and affiliated financial estimates were requested. However, the system deployed at MSP was not owned by the state. It is part of a service provided by the service vendor of the facility's inmate calling system. Therefore detailed cost information was not provided by this privately owned company. Moreover, managed access system cost factors will vary greatly by facility and the underlying cellular technology upon which a system operates. This case study provided a rural example whereby a single high-power cellular site provided coverage for the majority of the facility. The logistics associated with this type of installation are significantly different than a system using Distributed Antenna System technology (DAS), because DAS is based entirely on a network of low-power antennas distributed throughout the coverage area. The physical infrastructure required to support a DAS infrastructure is significantly more complex, and the associated costs to deploy will vary

significantly. DAS system manufacturers were/are hesitant to provide "budgetary" cost figures because of the significance of these differences. For this reason, cost estimates are not provided in this report. Given this high fidelity, any costs presented would likely not be generalizable.

Lastly, on-site engineering assessments were not a component of this project. The research team discussed such methodologies and determined that a number of system and facility-specific factors made any vulnerability assessment non-feasible. As an alternative, the research team employed social science process and outcome evaluation methods to describe how the managed access system operates, present information on implementation challenges, and explore and generate potential outcome metrics with the use of available administrative data.

Future research

It is beyond the scope of this study to take into account social factors contributing to the problem of contraband cell phones. The "why this is a problem" and "what are the root causes" questions cannot, unfortunately, be answered. As mentioned, the lack of privacy afforded to inmates via landline calls and the financial cost associated with these calls are plausible motivations for contraband cell phone use. However, further research is needed to explore the intention of calls conducted with contraband cell phones.

Relatedly, an exploration into the economics behind the contraband cell phone market could help quantify the problem and inform policy decisions. For example, if correctional officers and/or staff are smuggling phones for profit, it seems reasonable to assume that this cost is worth the risk of losing their legitimate job and facing likely criminal charges. Rational choice theory posits there should be an economic offset point where the proposed risk of smuggling is no-longer intriguing to an employee and they could be deterred from engaging in such behavior.

Furthermore, the current research does not explore possible technical vulnerabilities a managed access system may have. The question begs; do inmates learn how to "beat the system?" Conversations with Global Tel Link and Tecore representatives revealed rumors of inmates circumventing managed access through a variety of different dialing mechanisms and cell phone setting specifications. Exploring these possible vulnerabilities will require a unique methodology and, likely, wide-ranging sample of inmates across different facilities. Consideration should be given to the examination of confiscated cell phones to identify what features have, and have not, been disabled by the managed access system.

From an engineering and technical perspective, signal coverage to include coverage holes and coverage bleed over, should be examined in varying contexts. The deployment at MSP poses limited risk of cellular interference to nearby legitimate cell phone users. The rural setting includes a modest buffer between MSP grounds and public areas. In addition, the density of commercial cell sites in a rural setting is lower than in a typical urban setting. Installation of a managed access system in an urban environment will face a more daunting task to control and isolate signal bleed over because of the higher density of commercial cell sites combined with a small or non-existent buffer between the correctional facility and nearby public areas.

Lastly, future research on contraband cell phones should attempt to quantify victimization. This is not a straightforward task. Media stories often retrospectively highlight the most serious of offenses when they occur, but conversations with corrections practitioners indicate a more pervasive victimization enabled through cell phones. An informed estimate of contraband cell phone victimization could help to justify investment costs in contraband cell phone technologies, including managed access.

Caution for the Corrections Community

The corrections community must understand that managed access is not – and should not – be considered a silver bullet solution for the contraband cell phone problem. Cellular devices that cannot transmit a call or text pose potential harm in the correctional environment. Managed access should be utilized in conjunction with physical search and seizures of contraband cell phones. As noted above, multifunction device capabilities that fall outside of the scope of cellular communications simply cannot be managed with managed access technology and have to be mitigated via other means. Managed access technology serves as a tool to mitigate use of these devices by denying cellular service, diminishing the overall utility of smuggling these devices into a correctional facility. Clearly inmate use of multifunction device capabilities which fall outside of cellular communications requires mitigation using non-managed access system methods, to include physical intervention. Put simply, managed access technology should be viewed as supplemental to existing contraband policies and practices.

References

Aoki, K., & Downes, E. J. (2003). An Analysis of Young People's Use of and Attitudes Toward Cell Phones. *Telematics and Informatics, 20*(4), 349-364.

Bureau of Justice Statistics. (2013). *Correctional Populations in the United States, 2012*. NCJ 243936. U.S. Department of Justice. Washington, DC.

Burke, T. W. and Owen, S. S. (2010). Cell phones as prison contraband. *FBI Law Enforcement Bulletin*. July. Federal Bureau of Investigation.

California Council on Science and Technology. (2012). *Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons*. FEMA Grant Programs Directorate. U.S. Department of Homeland Security.

CorrectionsOne. (2015). S.C. towers will slow contraband, but cell phone jamming more effective. Retrieved from http://www.correctionsone.com/cell-phone-

jammers/articles/8348147-S-C-towers-will-slow-contraband-but-cell-phone-jamming-more-effective/

Entner, R. (2012). *The Wireless Industry: The Essential Engine of US Economic Growth*. Recon Analytics.

Epps, C. (2008). Commissioner's corner: Let this serve as a warning. Mississippi Department of Corrections. *The Resource*, 10(4), 1-16.

Federal Communications Commission. (2010). Contraband Cell Phone Use In Prisons Workshop/Webinar. Heritage Reporting Corporation. Retrieved from http://transition.fcc.gov/pshs/docs/summits/contraband-cell-use-transcript.pdf.

Federal Communications Commission (2005), *Sale or Use of Transmitters Designed to Prevent, Jam or Interfere with Cell Phone Communications is Prohibited in the United States.* Retrieved from: https://apps.fcc.gov/edocs_public/attachmatch/DA-05-1776A1.pdf

Federal Communications Commission. (2012). *Implementation of the pay telephone reclassification and compensation provisions of the Telecommunications Act of 1996 et al.* Hearings. Proceeding 12-375 retrieved from http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0711/DA-14-993A1.pdf

Federal Communications Commission. (2013). FCC Reduces High Long-Distance Calling Rates Paid by Inmates. Media Release. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/DOC-322749A1.pdf

Federal Communications Commission (NPRM 13-58, 2013). *Promoting Technological Solutions to Combat Contraband Wireless Devices Use in Correctional Facilities.* Retrieved from: https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-58A1.pdf

Federal Communications Commission Jamming (n.d.) *Jamming Tip Line*. Retrieved from: http://www.fcc.gov/encyclopedia/jammer-enforcement

Fitzpatrick, J. L. and Sanders, J. R. (2003). *Program Evaluation: Alternative Approaches and Practical Guidelines*. Allyn and Bacon. Upper Saddle River, NJ.

Hamel, J., Dufour, S. and Fortin, D. (1993). *Case Study Methods*. Newbury Park, CA. Sage.

Institute of Electrical and Electronics Engineers. (2014). *Evolution of Cell Phone Technology*. Global History Network. Retrieved from http://www.ieeeghn.org/wiki/index.php/Evolution_of_Cell_Phone_Technology

International Telecommunication Union. (2014). Mobile subscriptions near the 7‑billion mark: Does almost everyone have a phone? *ITU News*. Special Edition World Telecommunication Development Conference.

Johnson, W. J., Leach, M. P. and Liu, A. H. (1999). Theory testing using case studies in business-to-business research. *Industrial Marketing Management*, 28(3), 201-213.

Kennedy, M. M. (1979). Generalizing from single case studies. *Evaluation Review*, 3(4), 661-678.

King, N. (1994). The Qualitative Research Interview. In C. Cassell and G. Symon (Eds.), *Qualitative Methods in Organizational Research*, pp. 14-36. Sage. London.

Mississippi Department of Corrections. (n.d.). *Mississippi Department of Corrections 2013 Annual Report.* Jackson, MS: Mississippi Department of Corrections. Available at: http://www.mdoc.state.ms.us/Annual_report.htm.

Mississippi Department of Corrections. (2013). *Operational Cellblock: Locking Down Illegal Cell Phone Traffic*. Presentation. American Correctional Association. Houston, TX.

Mississippi Department of Corrections. (2014a). *Mississippi Department of Corrections Inmate Custody Population For Year's End 1990 – 2012*. Research and Statistics. Jackson, MS.

Mississippi Department of Corrections. (2014b). *The Resource*. A Publication of the Mississippi Department of Corrections. MDOC Making Strides. Retrieved from http://www.mdoc.state.ms.us/News%20Letters/2014NewsLetters/January2014.pdf

National Emergency Number Association. (2006). *Call Answering Standard/Model Recommendation*. National Emergency Number Association, Standard Operating Procedures Committing, Call-Taking Working Group. Document 56-005. Arlington, VA.

National Governors' Association Center for Best Practices. (2009). *State Strategies for Preventing Introduction and Use of Contraband Cell Phones in Prisons*, January,2009. Retrieved from http://www.asca.net/system/assets/attachments/864/NGA_Background_Paper_-_State_Strategies_for_Preventing_Introduction_and_Use_of_Contraband_Cell_Phones_1-27-2009.pdf?1280164386.

National Institute of Justice. (2010). *Plenary Panel: Cell Phones in Prisons*. NIJ Conference. Retrieved from http://nij.ncjrs.gov/multimedia/transcripts/audio-nijconf2010-plenary-cell-phones-transcript.htm

Nielsen. (2013). *Pay-As-You Phone: How Global Consumers Pay for Mobile*. NewsWire. Retrieved from http://www.nielsen.com/us/en/newswire/2013/how-global-consumers-pay-for-mobile.html

Pew Research Center. (2014). *Mobile Technology Fact Sheet*. Pew Research Internet Project. Retrieved from http://www.pewInternet.org/fact-sheets/mobile-technology-fact-sheet/.

Schofield, J. W. (2002). Increasing the generalizability of qualitative research. In, M. Huberman and M. B. Miles (Eds.), *The Qualitative Researcher's Companion: Classic and Contemporary Readings*, pp. 171-203. Sage. Thousand Oaks, CA.

State of Mississippi. (2012). Miss. Code § 47-5-193. *Title 47. Prisons and Prisoners; Probation and Parole. Chapter 5. Correctional System Alcoholic Beverages, Controlled Substance, Narcotic Drugs, Weapons, and other Contraband*. Retrieved from http://www.mdoc.state.ms.us/PDF%20Files/MissCode1972.pdf

Tecore Networks. (2014 Feb 20). Operating in a downtown Baltimore facility, Tecore releases unique details regarding its iNAC managed access capabilities. Retrieved from http://www.tecore.com/newsevents/release.cfm?newsID=205.

U.S. Department of Commerce. (2010). Contraband Cell Phones in Prisons: Possible Wireless Technology Solutions. Retrieved from http://www.ntia.doc.gov/files/ntia/publications/contrabandcellphonereport_december2010.pdf

U.S. Department of Labor and Statistics. (2013). *Occupational Employment and Wages, May 2013*. http://www.bls.gov/regions/southeast/news-release/occupationalemploymentandwages.htm

U.S. Department of Labor and Statistics. (2015). *Local Area Unemployment Statistics*. Retrieved from http://data.bls.gov/pdq/SurveyOutputServlet;jsessionid=85C515BA0B883F3F938F9A0D1B9F7C42.tc_instance5

U.S. Government Accountability Office. (2011). *Bureau of Prisons: Improved Evaluations and Increased Coordination Could Improve Cell Phone Detection*. Report to Congressional Committees. Report Number GAO-11-893. Washington, DC.

Washington Post. (2014 Feb 11). Governor: Phone security decreases jail violence. Washington Post. Retrieved from http://www.washingtonpost.com/local/omalley-to-announce-jail-phone-security -system/20140207/cac734e6-8fdd-11e3-878e-d76656564a01_print.html.

Worley, R. and Cheeseman, K. A. (2006). Guards as embezzlers: The consequences of "nonshareable problems" in prison settings. *Deviant Behavior*, 27(2), 203-222.

Yin, R. (1994). *Case Study Research: Design and Methods*. Second Edition. Sage. Beverly Hills, CA.

Appendix A: Examples of Contraband Cell Phone Activity

Contraband cell phones have been used for a variety of criminal activities inside and outside correctional facilities. While specific estimates of such activity have not been routinely collected or published, there is significant body of anecdotal evidence that the problem is widespread and poses a public safety problem. Table 13. illustrates some recent examples of alleged or noted criminal activities that have been associated with inmate use of contraband cell phones.

Table 13.Examples of Contraband Cell Phone Criminal Activity

State/ Country	Report Year	Criminal Act(s) Noted	Inside or outside prison	Reference URL
South Carolina	2010	Murder (attempted)	Outside	http://newsone.com/753345/prisoner-ordered-hit-outside-of-prison-with-smuggled-cell-phone/
Georgia	2011	Organized Inmate Uprisings	Inside	http://www.valdostadailytimes.com/local/x1331361164/Cell-phones-spark-Georgia-prison-unrest
North Carolina	2012	Kidnapping & Harass-ment	Outside	http://www.newsobserver.com/2014/04/11/3776630/kelvin-melton-imprisoned-for-life.html and/or http://www.theguardian.com/world/2014/apr/12/north-carolina-inmate-kidnapping-mobile-phone
Ohio (other locations mentioned)	2012	Multiple	Inside/ Outside	http://www.springfieldnewssun.com/news/news/cellphones-weapons-and-drugs-flood-ohio-prisons-1/nMySK/
South Carolina	2012	Smuggling, blackmail, harassment	Inside/ Outside	http://www.postandcourier.com/article/20120430/PC16/120439959 and http://www.postandcourier.com/article/20120430/PC16/120439971
Georgia	2013	Planning Violent Robberies	Outside	http://www.wsbtv.com/news/news/local/inmate-accused-planning-violent-crimes-prison/nXbw8/
Georgia	2013	Homicide	Inside	http://chronicle.augusta.com/news/2013-03-24/gangs-cell-phones-blamed-rise-homicides-georgia-prisons
Indiana	2013	Harassment	Outside	http://www.theindychannel.com/news/call-6-investigators/families-victims-targeted-by-indiana-state-prisoners-with-illegal-phones
Tennessee	2013	“violent crimes”	Outside	http://www.newschannel5.com/story/23631961/prisoners-confiscated-cell-phones-help-non-profit

State/ Country	Report Year	Criminal Act(s) Noted	Inside or outside prison	Reference URL
Georgia	2013	Prison Brawl Video	Inside	http://www.youtube.com/watch?v=C77wyuzh3oM
California	2014	Drug trafficking & Violent Crime	Outside	http://abc30.com/archive/9531064/
Maryland (Baltimore is mentioned)	2014	Smuggling etc.	Inside/ Outside	http://www.city-journal.org/2014/24_2_baltimore-correctional-services-corruption.html
Florida (other locations mentioned)	2014	Multiple	Inside/ Outside	http://tbo.com/news/crime/prisoners-use-of-smuggled-cellphones-on-rise-20140216/
International				
Brazil (Baltimore is mentioned)	2014	Murder	Outside	http://www.firstthings.com/web-exclusives/2014/04/prisoners-are-calling-whos-answering
Honduras	2014	Extortion	Outside	http://dialogo-americas.com/en_GB/articles/rmisa/features/regional_news/2014/05/30/honduras-seguridad

Appendix B: Semi-Structured Focus Group Protocol and Teleconference Protocols

Initial Focus Group Protocol – Mississippi Department of Corrections

Kick-Off: Introductions

a. Who we are (introductions, roles, background)
b. Overall charter and focus of NIJ
c. Work in corrections and communications
d. Assessment experience

1. Background of the project
   a. What motivated you to install the managed access system? Were there specific issues, a specific event, or general concern? Did you conduct a needs assessment or develop metrics to quantify the extent of the problem?
   b. What alternative approaches were implemented?
   c. What alternative approaches were considered?

2. System procurement
   a. How was the current system procured?
   b. What was the installation cost? Ongoing maintenance costs? Training costs? How are those costs funded?
   c. What was the timeline of procurement, installation, training, operation, etc.?

3. Technical operation of the system
   a. Physically view the system.

4. Operation of the managed access system
   a. Who installed the system? Who operates the system? How is the system maintained (hardware, software, data)?
   b. How are users trained?
   c. What are the relevant policies regarding cell phone use (employees, visitors)? How are these policies enforced?
   d. What is the criteria and procedure for classifying cell phones?

5. Operational impact
   a. What was your expectation for mitigating the issue that they were trying to address?
   b. What is your overall perception of system performance and impact?
   c. What would you change if you could (technical, policy, and legislative)?
   d. What data have you collected to date on system performance and system impact?

e. Overall what data is collected? Is that data available for analysis? How can that data be accessed? Is there any data sets for which we can view representative samples at this time?
f. How can we collect additional data if needed?

Debrief: Action steps for the future

Appendix C: Mississippi State Penitentiary Inmate Security Classifications

Security Level Classification	Definition
Minimum	Affords the offender a more relaxed atmosphere and extension of privileges and requires the ability to work satisfactorily with minimum supervision or security control.
Minimum: Community Minimum Status	Least security and supervision required of an offender. Usually this type offender works in the community.
Minimum: Non-Community Minimum Status	Least security and supervision required of an institutionalized offender and usually housed under minimum security circumstances. The offender may participate in activities on facility grounds without direct supervision, but must be supervised by trained correctional staff when off grounds.
Medium	Offender has displayed a desire to be considered responsible presents a moderate risk. Offenders are housed in a medium security facility and permitted to move about the housing unit or security work area, but are within direct observation of correctional staff. Offenders are under direct/constant armed correctional supervision when engaged in activities outside the perimeter of the correctional facility.
Close	Highest risk general population inmate and requires close supervision where the offender must be under positive security control at all times. The offender must be under armed supervision outside the perimeter.
Death Row	All male offenders sentenced to death in Mississippi are held in MSP's Unit 29.

Appendix D: MSP Managed Access System Infrastructure

The pictures included in this section were taken during a site visit made by the Engility team to the Mississippi State Penitentiary on May 31, 2012. These pictures are included to document specific aspects of the managed access installation.

As noted in the description of the installation, the system antennas were mounted on a water tower structure centrally located on the grounds of the MSP. Figure 16 shows the equipment shelter located at the base of the water tower structure. The equipment inside the shelter is shown in Figure 17, and the antennas, mounted on the structure, are shown in Figure 18

Figure 16. The MDOC Water Tower Equipment shelter

Figure 17. Equipment located in the MDOC Water Tower Equipment shelter

Figure 18. Antenna Equipment on the MDOC Water Tower